Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

Herausgegeben von

K. Hensel und H. Hasse

Band 174

In 4 Heften

Walter de Gruyter & Co.
vormals G. J. Göschen'sche Verlagshandlung — J. Guttentag, Verlagsbuchhandlung — Georg Reimer — Karl J. Trübner — Veit & Comp.
Berlin W 35 und Leipzig
1936

Archiv-Nr. 18 03 35

Druck von Walter de Gruyter & Co., Berlin W 35.

Printed in Germany.

Math. Lib.
Harv.

Inhaltsverzeichnis des Bandes 174.

Seite

Behrbohm, H., und **L. Rédei,** Der Euklidische Algorithmus in quadratischen Körpern 192

Eichler, Martin, Untersuchungen in der Zahlentheorie der rationalen Quaternionenalgebren 129

Grün, Otto, Beiträge zur Gruppentheorie. I. 1

Haenzel, G., Die Geometrie des linearen Strahlenkomplexes, gegründet auf seine Polarentheorie 226

Hasse, Helmut, und **Otto Schilling,** Die Normen aus einer normalen Divisionsalgebra über einem algebraischen Zahlkörper 248

Haupt, Otto, Zur Reinhardtschen Kennzeichnung der Kreisbogen 185

Kober, H., Funktionen, die den Potenzen der Riemannschen Zetafunktion verwandt sind, und Potenzreihen, die über den Einheitskreis nicht fortsetzbar sind 206

Lettenmeyer, Fritz, Über die sogenannte Hospitalsche Regel 246

Lubelski, S., Über Klassenzahlrelationen quadratischer Formen in quadratischen Körpern 160

Maruhn, Karl, Zur Theorie der Gleichgewichtsfiguren rotierender inhomogener Flüssigkeiten 68

Mayer, Anton E., Längste konvexe Kurven, die einem gegebenen konvexen Polygon umschrieben sind 125

Mises, R. v., Über allgemeine Quadraturformeln 56

Rédei, L., Über einige Mittelwertfragen im quadratischen Zahlkörper 15

Schilling, Otto F. G., Über die Darstellungen endlicher Gruppen 188

Sugawara, Masao, Zur Theorie der komplexen Multiplikation. I. 189

Teichmüller, Oswald, Operatoren im Wachsschen Raum 73

Witt, Ernst, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^l 237

Ausgabedaten der Hefte von Band 174.

Heft 1/2	ausgegeben am	1. November 1935
Heft 3	ausgegeben am	5. Februar 1936
Heft 4	ausgegeben am	4. März 1936

Beiträge zur Gruppentheorie. I.

Von *Otto Grün* in Berlin [1]).

$\mathfrak{G}$ sei durchweg eine Gruppe von endlicher Ordnung.

§ 1. Beziehungen zwischen Sylowgruppen zu verschiedenen Primzahlen.

Wir beweisen zunächst:

Satz 1. *Es sei $\mathfrak{A}$ eine abelsche in $\mathfrak{G}$ als Normalteiler enthaltene p-Gruppe, m der Rang von $\mathfrak{A}$, ferner $\mathfrak{L}$ eine l-Sylowgruppe von $\mathfrak{G}$ für eine Primzahl $l \neq p$ und m_l die Ordnung von l mod. p.*

Ist dann k der kleinste Exponent mit $\frac{m}{m_l} < l^k$, so ist $\mathfrak{A}$ mit der k-ten Ableitung $\mathfrak{L}^{(k)}$ von $\mathfrak{L}$ elementweise vertauschbar.

Beweis. a) Sei zunächst vorausgesetzt, daß $\mathfrak{A}$ vom Typus $(p, \ldots, p)$ ist. Dann ergibt sich die Behauptung leicht aus dem folgenden von mir in einer früheren Arbeit [2]) bewiesenen Satz:

Die l-Sylowgruppen der linearen Substitutionsgruppe vom Grade m im Galoisfeld $G(p^f)$ sind genau k-stufig metabelsch, wo k die in Satz 1 erklärte Bedeutung hat.

Um daraus die Behauptung von Satz 1 herzuleiten, betrachten wir die Darstellung von $\mathfrak{G}$ durch die Automorphismen, die $\mathfrak{A}$ bei Transformation mit Elementen aus $\mathfrak{G}$ erfährt. Dabei wird $\mathfrak{G}$ auf eine gewisse Untergruppe $\mathfrak{U}$ der Gruppe aller Automorphismen von $\mathfrak{A}$, also aller linearen Substitutionen vom Grade m in $G(p)$, homomorph abgebildet, und die Abbildung ist isomorph für die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ nach demjenigen Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$, der aus allen mit $\mathfrak{A}$ elementweise vertauschbaren Elementen von $\mathfrak{G}$ besteht. Nach dem angeführten Satz sind daher die l-Sylowgruppen von $\mathfrak{G}/\mathfrak{N} \cong \mathfrak{U}$ höchstens k-stufig metabelsch, d. h. ihre k-te Ableitung ist 1. Bei der Abbildung von $\mathfrak{G}$ auf $\mathfrak{G}/\mathfrak{N}$ geht aber jede l-Sylowgruppe $\mathfrak{L}$ von $\mathfrak{G}$ in eine l-Sylowgruppe $\mathfrak{L}\mathfrak{N}/\mathfrak{N}$ und jede Ableitung $\mathfrak{L}^{(i)}$ in die entsprechende Ableitung $\mathfrak{L}^{(i)}\mathfrak{N}/\mathfrak{N} \cong (\mathfrak{L}\mathfrak{N}/\mathfrak{N})^{(i)}$ über. Aus $(\mathfrak{L}\mathfrak{N}/\mathfrak{N})^{(k)} = 1$ folgt daher $\mathfrak{L}^{(k)} \leqq \mathfrak{N}$. Somit ist in der Tat $\mathfrak{L}^{(k)}$ elementweise mit $\mathfrak{A}$ vertauschbar.

b) Sei jetzt $\mathfrak{A}$ von beliebigem Typus. Wir betrachten die Untergruppen $\mathfrak{A}_p, \mathfrak{A}_{p^2}, \ldots$ aller derjenigen Elemente von $\mathfrak{A}$, deren p-te, p^2-te, ... Potenz 1 ist. Als charakteristische Untergruppen von $\mathfrak{A}$ sind $\mathfrak{A}_p, \mathfrak{A}_{p^2}, \ldots$ ebenfalls Normalteiler von $\mathfrak{G}$; ihr Rang ist sicher nicht größer als der Rang m von $\mathfrak{A}$.

Da $\mathfrak{A}_p$ vom Typus $(p, \ldots, p)$ ist, ist also nach dem in a) bereits Bewiesenen zunächst $\mathfrak{A}_p$ elementweise mit $\mathfrak{L}^{(k)}$ vertauschbar.

---

[1]) Für mannigfache Ratschläge bei der Gestaltung meiner Resultate zu der vorliegenden Arbeit bin ich Herrn H. Hasse zu Dank verpflichtet. Siehe insbesondere auch Fußnoten 5 und 8.

[2]) O. Grün, Über Substitutionsgruppen im Galoisfeld $G(p^f)$, dieses Journal **171** (1934), S. 172.

Ferner ist $\mathfrak{A}_{p^2}/\mathfrak{A}_p$ ein abelscher Normalteiler von $\mathfrak{G}/\mathfrak{A}_p$ vom Typus $(p, \ldots, p)$ von nicht höherem Rang als m. Nach a) (und einem entsprechenden Schluß wie oben bei $\mathfrak{N}$) ist also $\mathfrak{A}_{p^2}$ mit $\mathfrak{L}^{(k)}$ jedenfalls mod. $\mathfrak{A}_p$ elementweise vertauschbar. Sind daher A_{p^2}, L beliebige Elemente aus $\mathfrak{A}_{p^2}$, $\mathfrak{L}^{(k)}$, so gilt bei Transformation mit L

$$A_{p^2}^{L} = A_{p^2} \cdot A_p \quad \text{mit } A_p \text{ aus } \mathfrak{A}_p.$$

Daraus folgt durch p-malige Iteration, und weil $A_p^L = A_p$ bereits feststeht,

$$A_{p^2}^{L^p} = A_{p^2} \cdot A_p^p = A_{p^2}, \quad \text{da} \quad A_p^p = 1.$$

Da aber L als Element aus $\mathfrak{L}^{(k)} \leqq \mathfrak{L}$ eine zu p prime Ordnung hat, ergibt sich, daß auch L selbst mit A_{p^2} vertauschbar ist. Somit ist $\mathfrak{A}_{p^2}$ mit $\mathfrak{L}^{(k)}$ elementweise vertauschbar.

So fortfahrend ergibt sich die elementweise Vertauschbarkeit von $\mathfrak{L}^{(k)}$ mit $\mathfrak{A}$ als Schlußglied der aufsteigenden Kette $\mathfrak{A}_p, \mathfrak{A}_{p^2}, \ldots$. Damit ist Satz 1 bewiesen.

Satz 1 läßt sich zu einem entsprechenden Satz über mehrstufige p-Gruppen $\mathfrak{P}$ (statt der einstufigen $\mathfrak{A}$) verallgemeinern, die in $\mathfrak{G}$ als Normalteiler enthalten sind:

Satz 2. *Es sei $\mathfrak{P}$ eine in $\mathfrak{G}$ als Normalteiler enthaltene p-Gruppe, $\mathfrak{Z}_0=1, \mathfrak{Z}_1, \ldots, \mathfrak{Z}_r=\mathfrak{P}$ ihre aufsteigende Zentrenreihe ($\mathfrak{Z}_i/\mathfrak{Z}_{i-1}$ das Zentrum von $\mathfrak{P}/\mathfrak{Z}_{i-1}$; $i=1, \ldots, r$) und n_i der Rang von $\mathfrak{Z}_i/\mathfrak{Z}_{i-1}$. Ferner sei wieder $\mathfrak{L}$ eine l-Sylowgruppe von $\mathfrak{G}$ für eine Primzahl $l \neq p$ und m_l die Ordnung von l mod. p.*

Ist dann k der kleinste Exponent mit $\dfrac{n_i}{m_l} < l^{(k)}$ für alle $i=1, \ldots, r$, so ist $\mathfrak{P}$ mit $\mathfrak{L}^{(k)}$ elementweise vertauschbar.

Beweis. Als charakteristische Untergruppen von $\mathfrak{P}$ sind die $\mathfrak{Z}_i$ Normalteiler von $\mathfrak{G}$. Nach Satz 1 ist $\mathfrak{L}^{(k)}$ mit $\mathfrak{Z}_i$ jedenfalls mod. $\mathfrak{Z}_{i-1}$ elementweise vertauschbar. Daraus ergibt sich die Behauptung wie im Beweis zu Satz 1 unter b).

Für den Spezialfall, daß $\mathfrak{A}$ in Satz 1 sogar p-Sylowgruppe von $\mathfrak{G}$ ist, beweisen wir weiter:

Satz 3. *Hat $\mathfrak{G}$ als p-Sylowgruppe einen abelschen Normalteiler $\mathfrak{A}$ und ist der Rang von $\mathfrak{A}$ kleiner als die Grade aller nicht-abelschen absolut-irreduziblen Darstellungen von $\mathfrak{G}$, so ist $\mathfrak{A}$ mit der Kommutatorgruppe $\mathfrak{G}'$ elementweise vertauschbar.*

Beweis. a) Sei zunächst wieder $\mathfrak{A}$ vom Typus $(p, \ldots, p)$ und m der Rang von $\mathfrak{A}$. Wie im Beweis von Satz 1 unter a) betrachten wir die Darstellung Γ von $\mathfrak{G}$ vom Grade m in $G(p)$, die aus den Transformationsautomorphismen von $\mathfrak{A}$ mit Elementen aus $\mathfrak{G}$ entspringt. Sei Γ_0 ein absolut-irreduzibler Bestandteil von Γ und m_0 der Grad von Γ_0. Bekanntlich kann Γ_0 in einer endlichen algebraischen Erweiterung, also in einem gewissen $G(p^f)$ angenommen werden, und nach einem Satz von Speiser [3]) entspricht dann Γ_0 eine absolut-irreduzible Darstellung gleichen Grades m_0 im gewöhnlichen Sinne (in einem gewöhnlichen algebraischen Zahlkörper), weil hier die Ordnung der Darstellungsgruppe (nämlich $[\mathfrak{G}:\mathfrak{N}]$, wo $\mathfrak{N} \geqq \mathfrak{A}$ wie im Beweis zu Satz 1 erklärt ist) als Teiler von $[\mathfrak{G}:\mathfrak{A}]$ nach der gemachten Voraussetzung prim zu p ist. Nach der weiteren Voraussetzung ist somit Γ_0 abelsch (d. h. $m_0 = 1$). Dann werden aber alle Elemente von $\mathfrak{G}'$ durch 1 dargestellt, d. h. $\mathfrak{G}'$ ist mit $\mathfrak{A}$ elementweise vertauschbar.

b) Ist $\mathfrak{A}$ von beliebigem Typus, so schließt man wieder analog wie im Beweis zu Satz 1 unter b). An Stelle des dortigen L aus $\mathfrak{L}^{(k)}$ tritt hier ein C aus $\mathfrak{G}'$. Zwar hat hier C nicht notwendig eine zu p prime Ordnung, doch ist jedenfalls die Ordnung in bezug auf $\mathfrak{A}$ von C prim zu p, und das genügt für den dortigen Schluß.

---

[3]) A. Speiser, Gruppentheorie (2. Aufl., 1927), Satz 202.

§ 2. Die aufsteigende Zentrenreihe.

Das ist die Untergruppenreihe $\mathfrak{Z}_0 = 1, \mathfrak{Z}_1, \ldots, \mathfrak{Z}_r$, wo $\mathfrak{Z}_i/\mathfrak{Z}_{i-1}$ das Zentrum von $\mathfrak{G}/\mathfrak{Z}_{i-1}$ ist ($i = 1, \ldots, r$), und die dadurch abbricht, daß zuerst $\mathfrak{G}/\mathfrak{Z}_r$ das Zentrum 1 hat. Ist dabei $\mathfrak{Z}_r = \mathfrak{G}$, so heißt $\mathfrak{G}$ *nach aufsteigenden Zentren auflösbar.*

Bekanntlich ist jede p-Gruppe nach aufsteigenden Zentren auflösbar, und daher allgemeiner auch jedes direkte Produkt aus p-Gruppen, d. h. jede Gruppe $\mathfrak{G}$, die das direkte Produkt ihrer Sylowgruppen (für alle Primzahlen p) ist. Diese notwendige Bedingung für die Auflösbarkeit nach aufsteigenden Zentren ist auch hinreichend [4]):

Jede nach aufsteigenden Zentren auflösbare Gruppe $\mathfrak{G}$ ist das direkte Produkt ihrer Sylowgruppen.

Der von Hilton gegebene einfache Beweis mag hier kurz wiedergegeben werden, um dann daran eine weitere Bemerkung anzuknüpfen.

Sind S, T solche Elemente aus $\mathfrak{G}$, deren Kommutator $(S, T) = S^{-1}T^{-1}ST$ in $\mathfrak{Z}_1$ liegt, so gelten, wie man sofort bestätigt, die Relationen

$$(S, T)^k = (S^k, T) = (S, T^k) \quad \text{für jedes } k.$$

Haben also zudem S, T zueinander prime Ordnungen, so folgt $(S, T) = 1$, d. h. S und T sind miteinander vertauschbar. Wendet man dies, für zwei Elemente S, T zueinander primer Ordnungen aus $\mathfrak{G}$, auf $\mathfrak{G}/\mathfrak{Z}_{i-1}$ statt $\mathfrak{G}$ an, so hat man:

Liegt (S, T) in $\mathfrak{Z}_i$, so liegt (S, T) sogar in $\mathfrak{Z}_{i-1}$.

Ist also $\mathfrak{G} = \mathfrak{Z}_r$, so ergibt dies $(S, T) = 1$ für alle Elementpaare S, T zueinander primer Ordnungen aus $\mathfrak{G}$. Das liefert ohne weiteres die Behauptung.

Wir beweisen auf ähnlicher Grundlage:

Satz 4. *Ist $\mathfrak{Z}_2 > \mathfrak{Z}_1$, so ist $\mathfrak{G} > \mathfrak{G}'$; genauer: $\mathfrak{G}$ besitzt dann eine abelsche Faktorgruppe, die zu einer Untergruppe $\mathfrak{C} > 1$ von $\mathfrak{Z}_1$ isomorph ist.*

Beweis. Für jedes Z_2 in $\mathfrak{Z}_2$ und jedes S in $\mathfrak{G}$ gilt $(S, Z_2) \equiv 1 \bmod \mathfrak{Z}_1$, d. h. (S, Z_2) liegt in $\mathfrak{Z}_1$. Daraus ergibt sich, wie man sofort ähnlich wie oben bestätigt, die Relation

$$(ST, Z_2) = (S, Z_2)\,(T, Z_2)$$

für beliebige S, T in $\mathfrak{G}$. Durch die Kommutatoren (S, Z_2) wird also für jedes feste Z_2 aus $\mathfrak{Z}_2$ eine homomorphe Abbildung von $\mathfrak{G}$ auf eine gewisse Untergruppe $\mathfrak{C}_{Z_2}$ von $\mathfrak{Z}_1$ geliefert. Dabei ist $\mathfrak{C}_{Z_2} = 1$ dann und nur dann, wenn alle S aus $\mathfrak{G}$ mit Z_2 vertauschbar sind, d. h. wenn Z_2 in $\mathfrak{Z}_1$ liegt. Ist also $\mathfrak{Z}_2 > \mathfrak{Z}_1$, so gibt es ein Z_2 mit $\mathfrak{C}_{Z_2} = \mathfrak{C} > 1$. Das ergibt die Behauptung.

§ 3. Zusammenhang zwischen p-Sylowgruppen und Kommutatorfaktorgruppe.

A. p-normale Gruppen.

Wir nennen $\mathfrak{G}$ p-normal, wenn $\mathfrak{G}$ folgende Eigenschaft hat:

Das Zentrum $\mathfrak{Z}$ einer p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ ist Zentrum in jeder zu $\mathfrak{P}$ in $\mathfrak{G}$ Konjugierten, in der es überhaupt enthalten ist.

Die nachstehenden für das Folgende an sich entbehrlichen Ausführungen sollen dazu dienen, einen genaueren Einblick in die Bedeutung dieser Eigenschaft zu geben.

Sei $\mathfrak{N}$ der Normalisator von $\mathfrak{Z}$ in $\mathfrak{G}$. Natürlich ist $\mathfrak{P}$ in $\mathfrak{N}$ enthalten. Überdies enthält $\mathfrak{N}$ (für beliebiges $\mathfrak{G}$) genau diejenigen in $\mathfrak{G}$ zu $\mathfrak{P}$ konjugierten $\overline{\mathfrak{P}}$, die $\mathfrak{Z}$ als Zentrum enthalten.

---

[4]) H. Hilton, An introduction to the theory of groups, Oxford 1908, Chapter XIII, § 13.

Ist nämlich einerseits $\overline{\mathfrak{P}} \leqq \mathfrak{N}$, so ist $\overline{\mathfrak{P}} = \mathfrak{P}^N$ mit N in $\mathfrak{N}$, also $\mathfrak{Z}^N = \mathfrak{Z}$, und somit $\mathfrak{Z}$ auch Zentrum von $\overline{\mathfrak{P}}$. Und ist andrerseits $\mathfrak{Z}$ als Zentrum in der konjugierten $\overline{\mathfrak{P}} = \mathfrak{P}^S$ (S in $\mathfrak{G}$) enthalten, so ist $\mathfrak{Z}^S = \mathfrak{Z}$, also S in $\mathfrak{N}$, und somit $\overline{\mathfrak{P}} \leqq \mathfrak{N}$.

Hiernach kann die der p-Normalität zugrunde liegende Eigenschaft auch so formuliert werden:

Jede das Zentrum einer p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ enthaltende in $\mathfrak{G}$ zu $\mathfrak{P}$ Konjugierte ist im Normalisator $\mathfrak{N}$ von $\mathfrak{Z}$ in $\mathfrak{G}$ enthalten.

Für beliebiges $\mathfrak{G}$ ist $\mathfrak{Z}$ als gemeinsames Zentrum aller p-Sylowgruppen von $\mathfrak{N}$ eine charakteristische Untergruppe von $\mathfrak{N}$, und daher fällt $\mathfrak{N}$ mit seinem Normalisator in $\mathfrak{G}$ zusammen, d. h. $\mathfrak{N}^T = \mathfrak{N}$ gilt nur für T in $\mathfrak{N}$.

Auch das Kompositum $\mathfrak{R}$ aller p-Sylowgruppen von $\mathfrak{N}$ ist übrigens eine charakteristische Untergruppe von $\mathfrak{N}$, und zwar eine echte, wenn $\mathfrak{Z}$ nicht im Zentrum von $\mathfrak{N}$ liegt, denn $\mathfrak{Z}$ liegt im Zentrum von $\mathfrak{R}$. Die p-Sylowgruppen von $\mathfrak{N}$ sind bereits in $\mathfrak{R}$ konjugiert. Ist also N irgendein Element aus $\mathfrak{N}$, so existiert dazu ein Element R in $\mathfrak{R}$ mit $\mathfrak{P}^N = \mathfrak{P}^R$; dann ist NR^{-1} im Normalisator $\mathfrak{Q}$ von $\mathfrak{P}$ in $\mathfrak{G}$ gelegen, und somit gilt $\mathfrak{N} \leqq \mathfrak{Q}\mathfrak{R}$. Umgekehrt gilt neben $\mathfrak{R} \leqq \mathfrak{N}$ auch $\mathfrak{Q} \leqq \mathfrak{N}$, da $\mathfrak{Z}$ als charakteristische Untergruppe von $\mathfrak{P}$ Normalteiler von $\mathfrak{Q}$ ist. Somit gilt sogar $\mathfrak{N} = \mathfrak{Q}\mathfrak{R}$. Nach dem Isomorphiesatz folgt daraus $\mathfrak{N}/\mathfrak{R} \cong \mathfrak{Q}/\mathfrak{Q} \cap \mathfrak{R}$, wobei $\mathfrak{Q} \cap \mathfrak{R} \geqq \mathfrak{P}$ ist. Wir erwähnen, wie gesagt, alles dies nur beiläufig, um einen gewissen Einblick in die Bedeutung des Normalisators $\mathfrak{N}$ des Zentrums $\mathfrak{Z}$ von $\mathfrak{P}$ zu geben, der im folgenden eine wichtige Rolle spielt.

Wir beweisen nun zunächst zwei Hilfssätze über p-normale Gruppen; $\mathfrak{P}$, $\mathfrak{Z}$, $\mathfrak{N}$ haben dabei die vorstehend erklärte Bedeutung.

Hilfssatz 1. *Ist $\mathfrak{G}$ p-normal, so folgt aus $\mathfrak{Z}^T \leqq \mathfrak{N}$ mit T in $\mathfrak{G}$, daß T in $\mathfrak{N}$ liegt.*

Beweis. Ist $\mathfrak{Z}^T \leqq \mathfrak{N}$, so liegt $\mathfrak{Z}^T$ in einer p-Sylowgruppe $\mathfrak{P}^N$ von $\mathfrak{N}$ (N in $\mathfrak{N}$). Aus $\mathfrak{Z}^T \leqq \mathfrak{P}^N$ folgt wegen der vorausgesetzten p-Normalität von $\mathfrak{G}$, daß $\mathfrak{Z}^T$ das Zentrum $\mathfrak{Z}^N = \mathfrak{Z}$ von $\mathfrak{P}^N$ ist, also $\mathfrak{Z}^T = \mathfrak{Z}$. Wegen der Bedeutung von $\mathfrak{N}$ liegt somit T in $\mathfrak{N}$.

Folgerung. *Liegt T nicht in $\mathfrak{N}$, so ist die Anzahl der Linksklassen nach $\mathfrak{N}$ im Komplex $\mathfrak{Z}T\mathfrak{N}$ eine Potenz p^r mit $r \geqq 1$.*

Denn diese Anzahl ist bekanntlich gleich dem Index $[\mathfrak{Z}^T : (\mathfrak{Z}^T \cap \mathfrak{N})]$, also eine Potenz p^r, und nicht $p^0 = 1$, weil sonst $\mathfrak{Z}^T \leqq \mathfrak{N}$ wäre, also T nach Hilfssatz 1 in $\mathfrak{N}$ läge.

Hilfssatz 2. *Ist $\mathfrak{G}$ p-normal, so sind in $\mathfrak{G}$ konjugierte Elemente aus $\mathfrak{P}$ schon in $\mathfrak{N}$ konjugiert.*

Beweis. Sei $\overline{P} = P^S$ mit P, $\overline{P}$ in $\mathfrak{P}$ und S in $\mathfrak{G}$. Hier darf S durch ein beliebiges Linksvielfaches $N_P S$ mit N_P aus dem Normalisator $\mathfrak{N}_P$ von P in $\mathfrak{G}$ ersetzt werden. Wir zeigen, das es ein N_P in $\mathfrak{N}_P$ gibt, für das $N_P S = N$ in $\mathfrak{N}$ liegt.

Auf Grund der Bedeutung von $\mathfrak{Z}$ gilt

$$\mathfrak{N}_P \geqq \mathfrak{Z}$$

und entsprechend auch $\mathfrak{N}_{\overline{P}} = \mathfrak{N}_P^S \geqq \mathfrak{Z}$, also

$$\mathfrak{N}_P \geqq \mathfrak{Z}^{S^{-1}}.$$

Demnach existieren zwei p-Sylowgruppen von $\mathfrak{N}_P$, $\mathfrak{P}_0$ und $\mathfrak{P}_0^{N_P}$ mit N_P in $\mathfrak{N}_P$, derart, daß

$$\mathfrak{P}_0 \geqq \mathfrak{Z}$$

und $\mathfrak{P}_0^{N_P} \geqq \mathfrak{Z}^{S^{-1}}$, also

$$\mathfrak{P}_0^{N_P S} \geqq \mathfrak{Z}$$

ist. Da $\mathfrak{P}_0$ seinerseits in einer p-Sylowgruppe $\mathfrak{P}^*$ von $\mathfrak{G}$ enthalten ist, folgt aus der vorausgesetzten p-Normalität von $\mathfrak{G}$, daß $\mathfrak{Z}$ gleichzeitig Zentrum von $\mathfrak{P}^*$ und $\mathfrak{P}^{*N_P S}$ ist. Somit gilt

$$\mathfrak{Z}^{N_P S} = \mathfrak{Z}, \quad \text{d. h.} \quad N_P S = N \text{ in } \mathfrak{N}.$$

Damit ist Hilfssatz 2 bewiesen.

Wir betrachten nun die maximal-abelschen p-Faktorgruppen $\mathfrak{G}/\mathfrak{G}_0$ von $\mathfrak{G}$ und $\mathfrak{N}/\mathfrak{N}_0$ von $\mathfrak{N}$. Sie sind dadurch charakterisiert, daß $\mathfrak{G}_0/\mathfrak{G}'$ und $\mathfrak{N}_0/\mathfrak{N}'$ die maximalen Untergruppen zu p primer Ordnung von $\mathfrak{G}/\mathfrak{G}'$ und $\mathfrak{N}/\mathfrak{N}'$ sind.

Wir setzen

$$\mathfrak{N}_0^* = \mathfrak{N} \cap \mathfrak{G}_0, \quad \mathfrak{P}_0^* = \mathfrak{P} \cap \mathfrak{G}_0 = \mathfrak{P} \cap \mathfrak{N}_0^*, \quad \mathfrak{P}_0 = \mathfrak{P} \cap \mathfrak{N}_0.$$

Komplementär dazu hat man

$$\mathfrak{G} = \mathfrak{N}\mathfrak{G}_0 = \mathfrak{P}\mathfrak{G}_0, \quad \mathfrak{N} = \mathfrak{P}\mathfrak{N}_0^*, \quad \mathfrak{N} = \mathfrak{P}\mathfrak{N}_0.$$

Ist nämlich S ein beliebiges Element aus $\mathfrak{G}_0$ und bestimmt man dazu x aus den beiden miteinander verträglichen Kongruenzen

$$x \equiv 1 \text{ mod. } [\mathfrak{G} : \mathfrak{G}_0] \ (p\text{-Potenz}), \qquad x \equiv 0 \text{ mod. } [\mathfrak{G} : \mathfrak{P}] \ (\text{prim zu } p),$$

so gilt

$$S^x \equiv S \text{ mod. } \mathfrak{G}_0, \qquad S^x \text{ in } \mathfrak{P}.$$

Die Klassen von $\mathfrak{G}$ nach $\mathfrak{G}_0$ können also durch Elemente aus $\mathfrak{P}$ repräsentiert werden. Das bedeutet $\mathfrak{G} = \mathfrak{P}\mathfrak{G}_0$ und damit erst recht $\mathfrak{G} = \mathfrak{N}\mathfrak{G}_0$. Entsprechend folgt $\mathfrak{N} = \mathfrak{P}\mathfrak{N}_0^*$ und $\mathfrak{N} = \mathfrak{P}\mathfrak{N}_0$.

Nach dem Isomorphiesatz ergibt sich jetzt

$$\mathfrak{G}/\mathfrak{G}_0 \cong \mathfrak{N}/\mathfrak{N}_0^* \cong \mathfrak{P}/\mathfrak{P}_0^*, \quad \mathfrak{N}/\mathfrak{N}_0 \cong \mathfrak{P}/\mathfrak{P}_0.$$

Auf Grund der Bedeutung von $\mathfrak{N}_0$ ist hiernach

$$\mathfrak{N}_0 \leqq \mathfrak{N}_0^*, \quad \text{also auch} \quad \mathfrak{P}_0 \leqq \mathfrak{P}_0^*.$$

All dies stellt sich in einer geläufigen schematischen Veranschaulichung folgendermaßen dar:

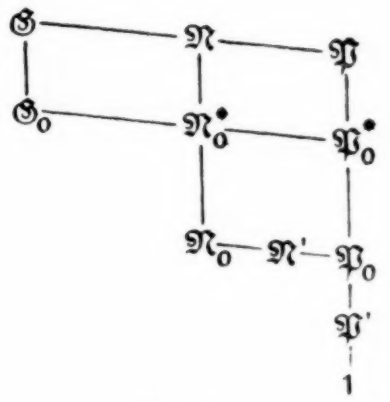

Fig. 1.

Dabei ist in der Tat, wie noch eingezeichnet, $\mathfrak{P}' \leqq \mathfrak{P}_0$, weil $\mathfrak{P}/\mathfrak{P}_0 \cong \mathfrak{N}/\mathfrak{N}_0$ abelsch ist, und $\mathfrak{P}_0 \leqq \mathfrak{N}'$, weil die Elemente aus $\mathfrak{P}_0 = \mathfrak{P} \cap \mathfrak{N}_0$ in bezug $\mathfrak{N}'$ einerseits p-Potenzordnung, andrerseits zu p prime Ordnung haben.

Unser Hauptsatz über p-normale Gruppen sagt nun aus, daß für p-normale $\mathfrak{G}$ in Wahrheit $\mathfrak{N}_0^* = \mathfrak{N}_0$, also auch $\mathfrak{P}_0^* = \mathfrak{P}_0$ gilt:

Satz 5. *Ist $\mathfrak{G}$ p-normal, so ist die maximal-abelsche p-Faktorgruppe $\mathfrak{G}/\mathfrak{G}_0$ von $\mathfrak{G}$ isomorph zur maximal-abelschen p-Faktorgruppe $\mathfrak{N}/\mathfrak{N}_0$ des Normalisators $\mathfrak{N}$ in $\mathfrak{G}$ des Zentrums $\mathfrak{Z}$ einer p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$.*

Beweis. a) Bekanntlich bildet (in jeder Gruppe $\mathfrak{G}$ für jede Untergruppe $\mathfrak{N}$) die *Verlagerung* $V_{\mathfrak{G}\to\mathfrak{N}}(\mathfrak{G})$ die Kommutatorfaktorgruppe $\mathfrak{G}/\mathfrak{G}'$ homomorph auf eine gewisse Untergruppe der Kommutatorfaktorgruppe $\mathfrak{N}/\mathfrak{N}'$ ab [5]). Betrachten wir hier die Verlagerung $V_{\mathfrak{G}\to\mathfrak{N}}(\mathfrak{G})$, kurz $V(\mathfrak{G})$, nur mod. $\mathfrak{N}_0$, so liefert sie eine homomorphe Abbildung von $\mathfrak{G}/\mathfrak{G}_0$ auf eine gewisse Untergruppe von $\mathfrak{N}/\mathfrak{N}_0$; denn aus

$$V(\mathfrak{G}_0)^n \equiv V(\mathfrak{G}_0^n) \equiv V(\mathfrak{G}') \equiv 1 \text{ mod. } \mathfrak{N}', \quad \text{wo} \quad n = [\mathfrak{G} : \mathfrak{G}_0] \text{ prim zu } p,$$

folgt nach der Bedeutung von $\mathfrak{N}_0$

$$V(\mathfrak{G}_0) \equiv 1 \text{ mod. } \mathfrak{N}_0 .$$

Auf Grund der bereits vor Satz 5 gemachten Ausführungen genügt es hiernach, zu zeigen, daß die homomorphe Abbildung $V(\mathfrak{G})$ mod. $\mathfrak{N}_0$ von $\mathfrak{G}/\mathfrak{G}_0$ auf die *volle* Gruppe $\mathfrak{N}/\mathfrak{N}_0$ erfolgt:

$$V(\mathfrak{G}) \equiv \mathfrak{N} \text{ mod. } \mathfrak{N}_0.$$

Wir zeigen, daß schon die Teilabbildung $V(\mathfrak{N})$ mod. $\mathfrak{N}_0$ auf die volle Gruppe $\mathfrak{N}/\mathfrak{N}_0$ erfolgt:

$$V(\mathfrak{N}) \equiv \mathfrak{N} \text{ mod. } \mathfrak{N}_0;$$

wegen $\mathfrak{N}_0 \leqq \mathfrak{N}_0^* \leqq \mathfrak{G}_0$ ist das sicher eine homomorphe Abbildung von $\mathfrak{N}/\mathfrak{N}_0$, und wegen $\mathfrak{N} = \mathfrak{P}\mathfrak{N}_0$ ist weiter sogar

$$V(\mathfrak{P}) \equiv V(\mathfrak{N}) \text{ mod. } \mathfrak{N}_0 ,$$

d. h. es genügt, die Teilabbildung $V(\mathfrak{P})$ mod. $\mathfrak{N}_0$ von $\mathfrak{P}/\mathfrak{P}_0$ zu betrachten und für sie

$$V(\mathfrak{P}) \equiv \mathfrak{N} \text{ mod. } \mathfrak{N}_0$$

nachzuweisen.

Diesen Nachweis erbringen wir dadurch, daß wir feststellen: für jedes Element A aus $\mathfrak{P}$ gilt eine Kongruenz der Form

$$\text{(V)} \qquad V(A) \equiv A^{1+hp} \text{ mod. } \mathfrak{N}_0 \text{ mit einem gewissen } h.$$

Dann geht nämlich bei der homomorphen Abbildung $V(\mathfrak{P})$ mod. $\mathfrak{N}_0$ von $\mathfrak{P}/\mathfrak{P}_0$ in $\mathfrak{N}/\mathfrak{N}_0$ jede Klasse in eine Klasse gleicher Ordnung, also nur die Hauptklasse in die Hauptklasse über, die Bilduntergruppe von $\mathfrak{N}/\mathfrak{N}_0$ hat also dieselbe Ordnung wie $\mathfrak{P}/\mathfrak{P}_0$ und ist somit wegen $\mathfrak{P}/\mathfrak{P}_0 \cong \mathfrak{N}/\mathfrak{N}_0$ zur vollen Gruppe $\mathfrak{N}/\mathfrak{N}_0$ isomorph.

b) Zum Beweis der Kongruenz (V) haben wir auf den Bildungsprozeß der Verlagerung $V(A)$ einzugehen. Durchläuft T ein beliebiges Repräsentantensystem $\mathfrak{T}$ der Linksklassen von $\mathfrak{G}$ nach $\mathfrak{N}$, also

$$\mathfrak{G} = \sum_T T\mathfrak{N},$$

so hat man ein Gleichungssystem

$$AT = T'N_T$$

mit eindeutig bestimmten T' aus $\mathfrak{T}$ und N_T aus $\mathfrak{N}$. Die Verlagerung $V(A)$ ist dann durch

$$V(A) \equiv \prod_T N_T \text{ mod. } \mathfrak{N}'$$

definiert. Die einzelnen Gleichungen $AT = T'N_T$ nennen wir im folgenden kurz die *Verlagerungsgleichungen* für A zu den Repräsentanten T.

[5]) Den Gedanken, bei diesem Beweise die ursprünglich von mir verwendeten monomialen Darstellungen durch die Verlagerung zu ersetzen, verdanke ich einer Mitteilung von H. Hasse. Dieser wurde seinerseits geleitet durch eine mündliche Mitteilung von E. Witt, wonach sich der klassische Beweis des Burnsideschen Satzes (s. u. Fußnote 6) in ganz entsprechender Weise einfacher und durchsichtiger gestalten läßt.

Wir unterscheiden nun drei Sorten von Repräsentanten T.

1) $T = 1$. Da A in $\mathfrak{P} \leqq \mathfrak{N}$ liegt, hat man dafür als Verlagerungsgleichung

$$AT = TA, \quad \text{und somit} \quad N_T = A$$

als Beitrag von $T = 1$ zu $V(A)$.

2) Repräsentanten T mit $T' = T$, d. h. A^T in $\mathfrak{N}$, aber T nicht in $\mathfrak{N}$. Jedem solchen Repräsentanten T entspricht gleich ein ganzes System von inäquivalenten Repräsentanten ZT mit der gleichen Eigenschaft, nämlich entsprechend der Zerlegung des Komplexes

$$\mathfrak{Z}T\mathfrak{N} = \sum_Z ZT\mathfrak{N}$$

mit gewissen Repräsentanten Z aus $\mathfrak{Z}$. In der Tat ist wegen der Bedeutung von $\mathfrak{Z}$ durchweg $A^{ZT} = A^T$ in $\mathfrak{N}$. Weil nun $\mathfrak{G}$ als p-normal vorausgesetzt wird, ist nach der obigen Folgerung aus Hilfssatz 1 die Anzahl der Repräsentanten ZT in jedem solchen System eine gewisse Potenz p^r mit $r \geqq 1$. Die zugehörigen Verlagerungsgleichungen sind

$$A \cdot ZT = ZT \cdot A^T, \quad \text{und daher durchweg} \quad N_{ZT} = A^T.$$

Jedes solche System ZT liefert also zu $V(A)$ einen Beitrag der Form

$$\prod_Z N_{ZT} = (A^T)^{p^r} \quad \text{mit einem gewissen } r \geqq 1.$$

3) Die übrigen Repräsentanten T, also die mit $T' \neq T$, d. h. A^T nicht in $\mathfrak{N}$, zerfallen in Zyklen entsprechend der Zyklenzerlegung der Permutation $T \to T'$. Da A in $\mathfrak{P}$ liegt, hat A^T in bezug auf $\mathfrak{N}$ eine Ordnung p^r; für die jetzt betrachten Repräsentanten T ist dabei $r \geqq 1$. Es bilden dann $T, AT, \ldots, A^{p^r-1}T$ ein System inäquivalenter Repräsentanten mit der gleichen Eigenschaft wie T, und diese Repräsentanten entsprechen gerade dem aus T entspringenden Zyklus. Dieser Zyklus ist also p^r-gliedrig, und die zugehörigen Verlagerungsgleichungen lauten

$$A \cdot A^i T = A^{i+1} T \cdot 1, \quad \text{also } N_{A^iT} = 1 \qquad (i = 0, 1, \ldots, p^r - 2)$$

$$A \cdot A^{p^r-1} T = T \cdot (A^{p^r})^T, \quad \text{also } N_{A^{p^r-1}T} = (A^{p^r})^T.$$

Daher liefert jeder solche Zyklus zu $V(A)$ einen Beitrag der Form

$$\prod_{i=0}^{p^r-1} N_{A^iT} = (A^{p^r})^T \quad \text{mit einem gewissen } r \geqq 1.$$

Insgesamt haben wir somit

$$V(A) \equiv A \cdot \prod_T{}' (A^T)^{p^r} \cdot \prod_T{}'' (A^{p^r})^T \text{ mod. } \mathfrak{N}',$$

wo T in Π' und Π'' gewisse Repräsentanten aus $\mathfrak{T}$ durchläuft und die zugeordneten (von T abhängigen) Exponenten $r \geqq 1$ sind.

Ein Faktor A^T aus Π' liegt nun als Element aus $\mathfrak{N}$ jedenfalls in einer gewissen p-Sylowgruppe $\mathfrak{P}^N (N \text{ in } \mathfrak{N})$ von $\mathfrak{N}$, und da auch A^N in $\mathfrak{P}^N$ liegt, folgt nach Hilfssatz 2 die Existenz eines $\overline{N}$ in $\mathfrak{N}$ mit $A^T = A^{N\overline{N}}$. Daher ist

$$A^T \equiv A \text{ mod. } \mathfrak{N}'.$$

Ganz entsprechend ergibt sich auch für die Faktoren aus Π''

$$(A^{p^r})^T \equiv A^{p^r} \text{ mod. } \mathfrak{N}'.$$

Zusammengenommen haben wir daher

$V(A) \equiv A \cdot \Pi' A^{p^r} \cdot \Pi'' A^{p^r}$ mod. $\mathfrak{N}'$, also sicher mod. $\mathfrak{N}_0$, mit gewissen $r \geqq 1$,

und daraus ergibt sich ohne weiteres die Behauptung (V). Damit ist Satz 5 bewiesen.

Aus Satz 5 läßt sich sehr einfach der folgende bekannte Satz von Burnside herleiten:

Ist die p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ im Zentrum ihres Normalisators $\mathfrak{N}$ in $\mathfrak{G}$ gelegen, so ist die maximal-abelsche p-Faktorgruppe $\mathfrak{G}/\mathfrak{G}_0$ von $\mathfrak{G}$ zu $\mathfrak{P}$ isomorph.

Unter dieser Voraussetzung ist nämlich in den bisherigen Bezeichnungen $\mathfrak{Z} = \mathfrak{P}$, also $\mathfrak{N}$ auch der Normalisator von $\mathfrak{Z}$, und $\mathfrak{G}$ ist trivialerweise p-normal.

Nach Satz 5 reduziert sich somit der Beweis des Burnsideschen Satzes auf den Nachweis, daß die maximal-abelsche p-Faktorgruppe $\mathfrak{N}/\mathfrak{N}_0$ von $\mathfrak{N}$ zu $\mathfrak{P}$ isomorph ist. Da nun $\mathfrak{P}$ im Zentrum von $\mathfrak{N}$ liegen soll, hat man für jedes Element A aus $\mathfrak{P}$ ohne weiteres

$$V_{\mathfrak{N}\to\mathfrak{P}}(A) = A^n, \quad \text{wo} \quad n = [\mathfrak{N}\colon \mathfrak{P}] \text{ prim zu } p.$$

Bei der homomorphen Abbildung $V_{\mathfrak{N}\to\mathfrak{P}}(\mathfrak{N})$ von $\mathfrak{N}/\mathfrak{N}'$ erfolgt also bereits die Teilabbildung $V_{\mathfrak{N}\to\mathfrak{P}}(\mathfrak{P})$ auf die volle Gruppe $\mathfrak{P}/\mathfrak{P}' = \mathfrak{P}$, umsomehr die ganze Abbildung. Das ergibt die Behauptung [6]).

Weitere Folgerungen aus Satz 5 ergeben sich, wenn man speziell voraussetzt, daß die p-Sylowgruppen von $\mathfrak{G}$ abelsch sind. Dann ist wieder $\mathfrak{Z} = \mathfrak{P}$, $\mathfrak{N}$ auch der Normalisator von $\mathfrak{P}$, und $\mathfrak{G}$ ist trivialerweise p-normal.

Wir haben so zunächst ohne weiteres aus Satz 5:

Satz 6. *Sind die p-Sylowgruppen von $\mathfrak{G}$ abelsch, so ist die maximal-abelsche p-Faktorgruppe von $\mathfrak{G}$ isomorph zur maximal-abelschen p-Faktorgruppe des Normalisators $\mathfrak{N}$ einer p-Sylowgruppe $\mathfrak{P}$.*

Wir folgern weiter aus Satz 5 die folgende Verallgemeinerung des Burnsideschen Satzes [7]):

Satz 7. *Sind die p-Sylowgruppen von $\mathfrak{G}$ abelsch, und ist $\mathfrak{A}$ eine Untergruppe einer von ihnen $\mathfrak{P}$, die im Zentrum des Normalisators $\mathfrak{N}$ von $\mathfrak{P}$ liegt, so besitzt $\mathfrak{G}$ eine zu $\mathfrak{A}$ isomorphe Faktorgruppe $\mathfrak{G}/\mathfrak{G}^*$.*

Beweis. Nach Satz 5 genügt es zu zeigen, daß $\mathfrak{N}$ eine zu $\mathfrak{A}$ isomorphe Faktorgruppe $\mathfrak{N}/\mathfrak{N}^*$ besitzt. Nun folgt aus der Zugehörigkeit von $\mathfrak{A}$ zum Zentrum von $\mathfrak{N}$ genau wie im obigen Beweis des Burnsideschen Satzes $V_{\mathfrak{N}\to\mathfrak{P}}(\mathfrak{A}) = \mathfrak{A}$. Dies besagt die Existenz einer zu $\mathfrak{A}$ isomorphen Faktorgruppe $\mathfrak{A}\mathfrak{N}'/\mathfrak{N}_0^*$ in $\mathfrak{N}/\mathfrak{N}'$ ($\mathfrak{N} \geqq \mathfrak{A}\mathfrak{N}' \geqq \mathfrak{N}_0^* \geqq \mathfrak{N}'$). Nach bekannten Sätzen über abelsche Gruppen besitzt dann auch $\mathfrak{N}/\mathfrak{N}'$ selbst eine zu $\mathfrak{A}$ isomorphe Faktorgruppe $\mathfrak{N}/\mathfrak{N}^*$ ($\mathfrak{N}^* \geqq \mathfrak{N}'$).

Schließlich folgern wir aus Satz 5:

Satz 8. *Sind die p-Sylowgruppen von $\mathfrak{G}$ abelsch, und ist $\mathfrak{A}$ eine Untergruppe einer von ihnen $\mathfrak{P}$, die Normalteiler des Normalisators $\mathfrak{N}$ von $\mathfrak{P}$ ist und für die $\mathfrak{P}/\mathfrak{A}$ im Zentrum von $\mathfrak{N}/\mathfrak{A}$ liegt, so besitzt $\mathfrak{G}$ eine zu $\mathfrak{P}/\mathfrak{A}$ isomorphe Faktorgruppe $\mathfrak{G}/\mathfrak{G}^*$.*

Beweis. Nach Satz 5 genügt es wieder zu zeigen, daß $\mathfrak{N}$ eine zu $\mathfrak{A}$ isomorphe Faktorgruppe $\mathfrak{N}/\mathfrak{N}^*$ besitzt. Dies ergibt sich aber ohne weiteres aus dem Burnsideschen Satz für $\mathfrak{N}/\mathfrak{A}$.

---

[6]) Der in Fußnote 5 erwähnte einfache Beweis des Burnsideschen Satzes von Witt entsteht, indem man die hier in zwei Schritte $V_{\mathfrak{G}\to\mathfrak{N}}$ und $V_{\mathfrak{N}\to\mathfrak{P}}$ zerlegte Verlagerungsbildung in dem einen Schritt $V_{\mathfrak{G}\to\mathfrak{P}}$ ausführt.

[7]) Wie ich nach Fertigstellung meiner Arbeit bemerkte, hat kürzlich auch H. Zassenhaus auf diese Verallgemeinerung hingewiesen, ohne allerdings den Beweis auszuführen; siehe dessen Arbeit: Über endliche Fastkörper, Abh. Math. Sem. Hamburg **11** (1935), S. 210. — Ein Spezialfall dieser Verallgemeinerung findet sich auch in der kürzlich erschienenen Arbeit von W. K. Turkin, Ein neues Kriterium der Einfachheit einer endlichen Gruppe, Math. Ann. **111** (1935), Theorem II. Auch das dortige Theorem I hat eine gewisse Verwandtschaft mit den Sätzen 5 und 9 dieser Arbeit.

Wir zeigen noch, daß keineswegs jede Gruppe p-normal ist. Zum Beispiel ist das Holomorph $\mathfrak{H}$ einer abelschen Gruppe $\mathfrak{A}$ vom n-gliedrigen Typus $(p, \ldots, p)$ für $n \geqq 2$ nicht p-normal. $\mathfrak{H}$ entsteht als verschränktes Produkt mit Faktorensystem 1 von $\mathfrak{A}$ mit seiner Automorphismengruppe $\mathfrak{S}$, d. h. indem man mit den formal gebildeten Produkten AS (A in $\mathfrak{A}$, S in $\mathfrak{S}$) nach den Regeln rechnet:

$$AS = A'S' \text{ nur für } A = A',\ S = S',$$

$$A^S = \text{Bild von } A \text{ beim Automorphismus } S.$$

$\mathfrak{S}$ wird vermöge einer Basis $A_1, \ldots, A_n$ von A als Gruppe aller regulären Matrizen n-ten Grades im Galoisfeld $G(p)$ isomorph dargestellt. Eine p-Sylowgruppe $\mathfrak{P}_{01}$ von $\mathfrak{S}$ wird dabei durch alle Matrizen gegeben, die 1 in und 0 über der Diagonale haben, für die also der zugeordnete Automorphismus P_1 die Gestalt

$$\begin{aligned} A_1^{P_1} &= A_1 \\ A_2^{P_1} &= A_1^{p_{21}} A_2 \\ &\cdots\cdots\cdots\cdots \\ A_n^{P_1} &= A_1^{p_{n1}} A_2^{p_{n2}} \cdots A_n \end{aligned}$$

hat. Dann ist $\mathfrak{P}_1 = \mathfrak{A}\mathfrak{P}_{01}$ eine p-Sylowgruppe von $\mathfrak{H} = \mathfrak{A}\mathfrak{S}$. Das Zentrum von $\mathfrak{P}_1$ ist, wie leicht zu sehen, die durch A_1 erzeugte Untergruppe $\mathfrak{A}_1$ von $\mathfrak{A}$. Dieses Zentrum $\mathfrak{A}_1$ von $\mathfrak{P}_1$ ist nun als Untergruppe des Normalteilers $\mathfrak{A}$ von $\mathfrak{H}$ in *jeder* p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{H}$ enthalten. $\mathfrak{A}_1$ ist aber in allen und nur denjenigen p-Sylowgruppen $\mathfrak{P}$ von $\mathfrak{H}$ Zentrum, die in der Untergruppe $\mathfrak{H}_1 = \mathfrak{A}\mathfrak{S}_1$ von $\mathfrak{H}$ liegen, wo $\mathfrak{S}_1$ die Untergruppe derjenigen Automorphismen S_1 von $\mathfrak{A}$ ist, die A_1 festlassen, also

$$\begin{aligned} A_1^{S_1} &= A_1 \\ A_2^{S_1} &= A_1^{s_{21}} \cdots A_n^{s_{2n}} \\ &\cdots\cdots\cdots\cdots \\ A_n^{S_1} &= A_1^{s_{n1}} \cdots A_n^{s_{nn}}. \end{aligned}$$

Für $n \geqq 2$ gibt es aber auch nicht in der Untergruppe $\mathfrak{H}_1$ liegende p-Sylowgruppen von $\mathfrak{H}$, zum Beispiel die Gruppe $\mathfrak{P}_1^* = \mathfrak{A}\mathfrak{P}_{01}^*$, wo $\mathfrak{P}_{01}^*$ durch alle Matrizen P_1^* mit 1 in und 0 *unter* der Diagonale gegeben ist. In einer p-Sylowgruppe $\mathfrak{P}_1^*$ ist also $\mathfrak{A}_1$ zwar enthalten, aber nicht Zentrum. Das Zentrum von $\mathfrak{P}_1^*$ ist vielmehr die durch $\mathfrak{A}_n$ erzeugte Untergruppe $\mathfrak{A}_n$ von $\mathfrak{A}$.

B. Beliebige Gruppen.

Auch für beliebige Gruppen läßt sich die maximal-abelsche p-Faktorgruppe durch die p-Sylowgruppen charakterisieren, wenn auch nicht mehr in ganz so einfacher Form wie für p-normale Gruppen.

Es sei $\mathfrak{P}$ eine p-Sylowgruppe von $\mathfrak{G}$ und $\mathfrak{N}$ ihr Normalisator in $\mathfrak{G}$ ($\mathfrak{N}$ ist also jetzt nicht mehr der Normalisator nur des Zentrums von $\mathfrak{P}$). Wir übernehmen die vor Satz 5 eingeführten und in Fig. 1 schematisch dargestellten Bezeichnungen. Alles dort Entwickelte gilt ohne weiteres auch bei der jetzigen Bedeutung von $\mathfrak{N}$. Während aber dort, wie in Satz 5 festgestellt, $\mathfrak{N}_0^*$, $\mathfrak{P}_0^*$ mit $\mathfrak{N}_0$, $\mathfrak{P}_0$ zusammenfallen, ist das hier im allgemeinen nicht der Fall. Es handelt sich für uns darum, die zunächst von $\mathfrak{G}$ aus durch Durchschnittsbildungen (also von oben her) definierten Gruppen $\mathfrak{N}_0^*$, $\mathfrak{P}_0^*$ auch von $\mathfrak{N}$, $\mathfrak{P}$ aus durch Kompositumsbildungen (von unten her) zu charakterisieren. Dazu bilden wir das Kompositum

$$\Pi = \prod_{S \text{ in } \mathfrak{G}} (\mathfrak{P} \cap \mathfrak{P}'^S)$$

und damit weiter

$$\overline{\mathfrak{P}} = \Pi\mathfrak{P}_0, \qquad \overline{\mathfrak{N}} = \Pi\,\mathfrak{N}_0 = \overline{\mathfrak{P}}\mathfrak{N}_0.$$

Jedenfalls gilt

$$\overline{\mathfrak{P}} \leqq \mathfrak{P}_0^*, \quad \text{also} \quad \overline{\mathfrak{N}} \leqq \mathfrak{N}_0^*;$$

denn es ist durchweg $\mathfrak{P} \cap \mathfrak{P}'^S \leqq \mathfrak{P} \cap \mathfrak{G}' \leqq \mathfrak{P} \cap \mathfrak{G}_0 = \mathfrak{P}_0^*$. Wir haben also jedenfalls folgendes Schema:

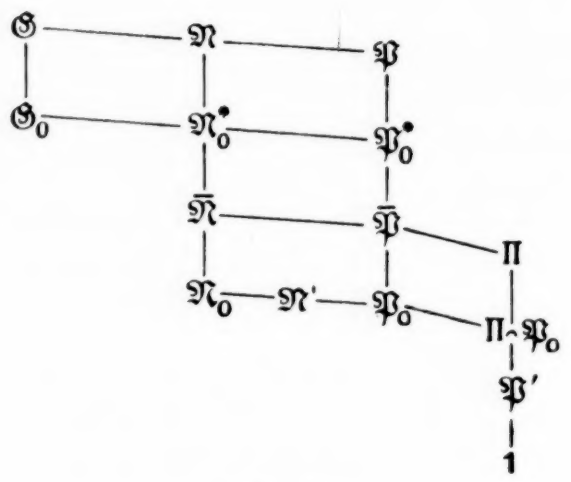

Fig. 2.

Weil jetzt $\mathfrak{P}$ Normalteiler von $\mathfrak{N}$ ist, sind auch $\mathfrak{P}_0^*$, $\overline{\mathfrak{P}}$, $\mathfrak{P}_0$ (und seiner Definition nach auch Π) Normalteiler von $\mathfrak{N}$, und überdies sind $\mathfrak{P}_0^*$, $\overline{\mathfrak{P}}$, $\mathfrak{P}_0$ die (einzigen) p-Sylowgruppen von $\mathfrak{N}_0^*$, $\overline{\mathfrak{N}}$, $\mathfrak{N}_0$ und $\mathfrak{N}'$.

Wir beweisen nun daß in Wahrheit $\overline{\mathfrak{N}} = \mathfrak{N}_0^*$, also auch $\overline{\mathfrak{P}} = \mathfrak{P}_0^*$ gilt:

Satz 9. *Es sei $\mathfrak{P}$ eine p-Sylowgruppe von $\mathfrak{G}$, $\mathfrak{N}$ ihr Normalisator in $\mathfrak{G}$, $\mathfrak{P}_0$ die p-Sylowgruppe der Kommutatorgruppe $\mathfrak{N}'$,*

$$\Pi = \prod_{S \text{ in } \mathfrak{G}} (\mathfrak{P} \cap \mathfrak{P}'^S)$$

das Kompositum der Durchschnitte von $\mathfrak{P}$ mit allen in $\mathfrak{G}$ zu $\mathfrak{P}'$ Konjugierten, und

$$\overline{\mathfrak{P}} = \Pi\mathfrak{P}_0\,.$$

Die maximal-abelsche p-Faktorgruppe $\mathfrak{G}/\mathfrak{G}_0$ von $\mathfrak{G}$ ist isomorph zu der Faktorgruppe $\mathfrak{P}/\overline{\mathfrak{P}}$ von $\mathfrak{P}$.

$\mathfrak{G}/\mathfrak{G}_0$ ist überdies isomorph zu derjenigen Faktorgruppe $\mathfrak{N}/\overline{\mathfrak{N}}$ der maximal-abelschen p-Faktorgruppe $\mathfrak{N}/\mathfrak{N}_0$ von $\mathfrak{N}$, die durch

$$\overline{\mathfrak{N}} = \Pi\,\mathfrak{N}_0 = \overline{\mathfrak{P}}\mathfrak{N}_0$$

geliefert wird [8]).

Beweis. Wie aus den Vorbemerkungen hervorgeht, genügt es zu zeigen, daß $[\mathfrak{G} : \mathfrak{G}_0] \geqq [\mathfrak{P} : \overline{\mathfrak{P}}]$ ist. Wir zeigen das dadurch, daß wir die Existenz einer zu $\mathfrak{P}/\overline{\mathfrak{P}}$ isomorphen Faktorgruppe $\mathfrak{G}/\mathfrak{G}_m$ von $\mathfrak{G}/\mathfrak{G}_0$ nachweisen. $\mathfrak{G}_m$ wird sich als Schlußglied einer absteigenden Untergruppenkette $\mathfrak{G}_1, \ldots, \mathfrak{G}_m$ herausstellen, entsprechend der abfallend geordneten Reihe $p^{k_1}, \ldots, p^{k_m}$ $(k_1 \geqq \cdots \geqq k_m)$ der Invarianten der abelschen Gruppe $\mathfrak{P}/\overline{\mathfrak{P}} \cong \mathfrak{N}/\overline{\mathfrak{N}}$.

a) Wir zeigen zunächst, daß $\mathfrak{G}/\mathfrak{G}_0$ einen direkten Faktor $\mathfrak{G}_1/\mathfrak{G}_0$ mit zyklischer Faktorgruppe $\mathfrak{G}/\mathfrak{G}_1$ der Ordnung p^{k_1} hat.

---

[8]) Diesem Satz und seinem Beweis hat Herr Hasse die vorliegende Form gegeben. Ich habe mich ursprünglich darauf beschränkt, bei den gemachten Voraussetzungen eine zyklische p-Faktorgruppe nachzuweisen.

Sei dazu A_1 ein Element aus $\mathfrak{P}$ von der maximalen Ordnung p^{k_1} mod. $\overline{\mathfrak{P}}$, das möglichst niedrige absolute Ordnung hat. Dann ist $\{A_1\overline{\mathfrak{P}}\}/\overline{\mathfrak{P}}$ direkter Faktor der Ordnung p^{k_1} von $\mathfrak{P}/\overline{\mathfrak{P}}$; es existiert also (mindestens) ein dazu komplementärer direkter Faktor $\mathfrak{P}_1/\overline{\mathfrak{P}}$ (derart, daß die ganze Gruppe $\mathfrak{P}/\overline{\mathfrak{P}}$ das direkte Produkt der beiden genannten komplementären Faktoren ist). Natürlich ist dann auch $\{A_1\overline{\mathfrak{N}}\}/\overline{\mathfrak{N}}$ direkter Faktor derselben Ordnung p^{k_1} von $\mathfrak{N}/\overline{\mathfrak{N}}$, und $\mathfrak{N}_1/\overline{\mathfrak{N}}$ mit $\mathfrak{N}_1 = \mathfrak{P}_1\overline{\mathfrak{N}}$ ist ein dazu komplementärer Faktor.

Wir betrachten nun, ähnlich wie im Beweis von Satz 5, die durch die Verlagerung $V_{\mathfrak{G}\to\mathfrak{N}}(\mathfrak{P})$, kurz $V(\mathfrak{P})$, mod. $\overline{\mathfrak{N}}$ gelieferte homomorphe Abbildung von $\mathfrak{P}/\overline{\mathfrak{P}}$ in $\mathfrak{N}/\overline{\mathfrak{N}}$ und zeigen nachstehend unter b) und c), daß für das oben definierte Element A_1 eine Kongruenz der Form

$$(V_1) \qquad V(A_1) \equiv A^{1+h_1 p} \text{ mod. } \mathfrak{N}_1$$

mit einem gewissen h_1 gilt.

b) Zum Nachweis von (V_1) leiten wir zunächst eine Kongruenz für die Verlagerung $V(A)$ eines beliebigen Elements A aus $\mathfrak{P}$ her, die wir nachher auf A_1 und später auch auf die den weiteren Invarianten $p^{k_2}, \ldots, p^{k_m}$ in bestimmter Weise zuzuordnenden Elemente $A_2, \ldots, A_m$ anwenden werden.

Wir legen dazu die Repräsentanten der Linksklassen von $\mathfrak{G}$ nach $\mathfrak{N}$ hier etwas anders fest als oben im Beweis von Satz 5. Ausgehend von der Doppelzerlegung

$$\mathfrak{G} = \sum_T \mathfrak{P}T\mathfrak{N}, \qquad T \text{ aus } \mathfrak{G}$$

und der weiteren Zerlegung

$$\mathfrak{P}T\mathfrak{N} = \sum_P PT\mathfrak{N}, \qquad P \text{ aus } \mathfrak{P}$$

jedes einzelnen ihrer Komplexe, nehmen wir als Repräsentanten der Linksklassen von $\mathfrak{G}$ nach $\mathfrak{N}$ die Repräsentantenprodukte PT. Wegen $A\mathfrak{P}T\mathfrak{N} = \mathfrak{P}T\mathfrak{N}$ für A in $\mathfrak{P}$ ist die in den Verlagerungsgleichungen für A auftretende Permutation dieser Repräsentanten so beschaffen, daß die jedem einzelnen Komplex $\mathfrak{P}T\mathfrak{N}$ entsprechenden Repräsentanten PT (T fest) nur untereinander permutiert werden. Dementsprechend stellt sich die Verlagerung $V(A)$, nach Beiträgen der einzelnen Komplexe $\mathfrak{P}T\mathfrak{N}$ zerlegt, folgendermaßen dar:

$$V(A) \equiv A \cdot \prod_T \Big(\prod_P{}' A^{PT} \cdot \prod_P{}'' (A^{p^r})^{PT} \Big) \text{ mod. } \mathfrak{N}'.$$

Dabei ist der Beitrag A des Hauptkomplexes $\mathfrak{N}\mathfrak{P} = \mathfrak{N}$ vorweggenommen, dann folgt das Produkt über die Beiträge der übrigen Komplexe $\mathfrak{P}T\mathfrak{N}$, für die also T nicht in $\mathfrak{N}$ liegt. Innerhalb jedes solchen Beitrags sind in $\prod'$ diejenigen Repräsentanten PT berücksichtigt, für die A^{PT} in $\mathfrak{N}$ (und dann hier sogar in der einzigen p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{N}$) liegt, und in $\prod''$ dann die übrigen Repräsentanten PT, die sich wieder zu p^r-gliedrigen Zyklen mit $r \geqq 1$ zusammenfassen lassen, wo jeweils zuerst $(A^{p^r})^{PT}$ in $\mathfrak{N}$ liegt.

Für jedes T (nicht in $\mathfrak{N}$) ist die Anzahl der Faktoren in $\prod'$ ein Multiplum up. Denn die Gesamtanzahl der zu T gehörigen PT ist gleich dem Index $[\mathfrak{P}^T : (\mathfrak{P}^T \cap \mathfrak{N})]$, also eine Potenz $p^{\bar{r}}$, und zwar mit $\bar{r} \geqq 1$, da sonst $\mathfrak{P}^T \leqq \mathfrak{N}$ wäre, also T nach der Bedeutung von $\mathfrak{N}$ in $\mathfrak{N}$ läge. Die Anzahl der Faktoren in $\prod'$ ist dann gleich $p^{\bar{r}} - \sum_P{}'' p^r$, wo über die einzelnen Zyklenzahlen p^r zu den P in $\prod''$ summiert ist; sie ist also in der Tat ein Multiplum von p.

Ferner gilt für irgend zwei in $\boldsymbol{\Pi}'$ auftretende Repräsentanten P_1T, P_2T

$$A^{P_1T} \equiv A^{P_2T} \text{ mod. } \Pi, \quad \text{also sicher mod. } \overline{\mathfrak{N}}.$$

Denn das läuft auf die Zugehörigkeit zu Π des Elementes

$$P = A^{P_1T}A^{-P_2T} = (A \cdot P_1P_2^{-1} \cdot A^{-1} \cdot P_2P_1^{-1})^{P_1T}$$

hinaus. Dies Element P liegt aber wegen des ersten Ausdrucks nach unserer Konstruktion in $\mathfrak{P}$ und wegen des zweiten Ausdrucks in $\mathfrak{P}'^{P_1T} = \mathfrak{P}'^{T}$, zusammengenommen also in $\mathfrak{P} \cap \mathfrak{P}'^{T} \leqq \Pi$.

Hiernach ergibt sich die für jedes A aus $\mathfrak{P}$ gültige Kongruenz

$$\text{(K)} \qquad V(A) \equiv A \cdot \prod_{T} \left((A^{PT})^{up} \cdot \boldsymbol{\Pi}''(A^{p^r})^{PT} \right) \text{ mod. } \overline{\mathfrak{N}}$$

mit gewissen u und gewissen $r \geqq 1$.

c) Wir wenden (K) jetzt auf das oben ausgewählte Element A_1 an. Für die in (K) auftretenden zu $\mathfrak{P}$ gehörigen Faktoren A_1^{PT}, $(A_1^{p^r})^{PT}$ hat man bei der oben erklärten Bedeutung von $\mathfrak{P}_1$ und $\mathfrak{N}_1$ Kongruenzen

$$A_1^{PT} \equiv A_1^{x}, \ (A_1^{p^r})^{PT} \equiv A_1^{y} \text{ mod. } \mathfrak{P}_1, \text{ also auch mod. } \mathfrak{N}_1.$$

Dabei ist durchweg $y = y_0 p$. Denn wäre $y \not\equiv 0$ mod. p, so hätte das zu $\mathfrak{P}$ gehörige Element $(A_1^{p^r})^{PT}$ mod. $\mathfrak{P}_1$ und somit erst recht mod. $\overline{\mathfrak{P}}$ die maximale in $\mathfrak{P}/\overline{\mathfrak{P}}$ vorkommende Ordnung p^{k_1}, während wegen $r \geqq 1$ seine absolute Ordnung niedriger als die von A_1 ist; das widerspricht aber der obigen Auswahl von A_1.

Hiernach ergibt sich aus (K) für das Element A_1 eine Kongruenz

$$V(A_1) \equiv A_1 \cdot A_1^{p\Sigma ux} \cdot A_1^{p\Sigma y_0} \text{ mod. } \mathfrak{N}_1$$

von der oben in (V_1) behaupteten Form.

d) Die Kongruenz (V_1) besagt mit Rücksicht auf die Tatsache $V(\mathfrak{G}_0) \equiv 1$ mod. $\mathfrak{N}_0$, also sicher mod. $\mathfrak{N}_1$, daß das Element A_1 mod. $\mathfrak{G}_0$ mindestens die Ordnung p^{k_1} hat. Da aber wegen $\mathfrak{G}/\mathfrak{G}_0 \cong \mathfrak{P}/\mathfrak{P}_0^*$ und $\mathfrak{P}_0^* \geqq \overline{\mathfrak{P}}$ die maximale Ordnung in $\mathfrak{G}/\mathfrak{G}_0$ höchstens gleich p^{k_1} ist, ergibt sich, daß A_1 mod. $\mathfrak{G}_0$ genau von der Ordnung p^{k_1} ist und daß p^{k_1} die maximale Ordnung in $\mathfrak{G}/\mathfrak{G}_0$ ist. Hiernach ist die Untergruppe $\{A_1\mathfrak{G}_0\}/\mathfrak{G}_0$ ein direkter Faktor der Ordnung p^{k_1} von $\mathfrak{G}/\mathfrak{G}_0$. Es existiert also ein zu ihr komplementärer direkter Faktor $\mathfrak{G}_1/\mathfrak{G}_0$ derart, daß $\mathfrak{G}/\mathfrak{G}_1$ zyklisch von der Ordnung p^{k_1} ist. Damit ist die zu Beginn ausgesprochene Behauptung bewiesen.

e) Zur Fortführung und Vollendung unseres schrittweise vorgehenden Beweises definieren wir von der erhaltenen Untergruppe $\mathfrak{G}_1$ aus Gruppen $\mathfrak{N}_1^*$, $\mathfrak{P}_1^*$ ganz analog wie von $\mathfrak{G}_0$ aus $\mathfrak{N}_0^*$, $\mathfrak{P}_0^*$ definiert waren, also

$$\mathfrak{N}_1^* = \mathfrak{N} \cap \mathfrak{G}_1, \qquad \mathfrak{P}_1^* = \mathfrak{P} \cap \mathfrak{G}_1.$$

Wegen $\mathfrak{G}_1 \geqq \mathfrak{G}_0$ gilt dann

$$\mathfrak{N}_1^* \geqq \mathfrak{N}_0^*, \qquad \mathfrak{P}_1^* \geqq \mathfrak{P}_0^*,$$

Unser in Fig. 2 gegebenes Schema füllt sich dementsprechend folgendermaßen auf:

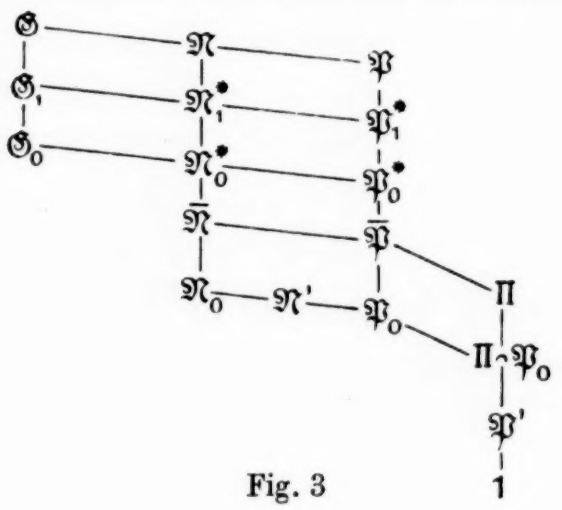

Fig. 3

Die Gruppen $\mathfrak{P}_1^*, \mathfrak{N}_1^*$ haben dieselbe Eigenschaft, wie die unter a) (von unten her) eingeführten Gruppen $\mathfrak{P}_1, \mathfrak{N}_1$; die Freiheit in der Wahl der letzteren ist durch unsere an $\mathfrak{G}_1$ geknüpfte Definition (von oben her) der ersteren auf die Freiheit in der Wahl von $\mathfrak{G}_1$ beschränkt worden.

Da insbesondere $[\mathfrak{G}_1 : \mathfrak{N}_1^*] = [\mathfrak{G} : \mathfrak{N}]$ ist, ist jedes Repräsentantensystem für die Linksklassen von $\mathfrak{G}_1$ nach $\mathfrak{N}_1^*$ auch ein solches für die Linksklassen von $\mathfrak{G}$ nach $\mathfrak{N}$. Speziell ist daher ein der Doppelzerlegung von $\mathfrak{G}_1$ nach $\mathfrak{P}_1^*, \mathfrak{N}_1^*$ angepaßtes Repräsentantensystem von $\mathfrak{G}_1$ nach $\mathfrak{N}_1^*$ auch ein der Doppelzerlegung von $\mathfrak{G}$ nach $\mathfrak{P}, \mathfrak{N}$ angepaßtes Repräsentantensystem von $\mathfrak{G}$ nach $\mathfrak{N}$. Die Repräsentanten P, T in b) lassen sich also innerhalb $\mathfrak{P}_1^*, \mathfrak{G}_1$ wählen.

Die maximale Ordnung in $\mathfrak{P}_1^*/\overline{\mathfrak{P}}$ ist nach unserer Konstruktion gleich der zweiten Invariante p^{k_2} von $\mathfrak{P}/\overline{\mathfrak{P}}$. Sei demgemäß jetzt A_2 ein Element aus $\mathfrak{P}_1$ von der maximalen Ordnung p^{k_2} mod. $\overline{\mathfrak{P}}$, das wieder möglichst niedrige absolute Ordnung hat. Ferner sei $\mathfrak{P}_2/\overline{\mathfrak{P}}$ ein zu $\{A_2\overline{\mathfrak{P}}\}/\overline{\mathfrak{P}}$ komplementärer direkter Faktor von $\mathfrak{P}_1^*/\overline{\mathfrak{P}}$ und $\mathfrak{N}_2 = \mathfrak{P}_2\overline{\mathfrak{N}}$, also $\mathfrak{N}_2/\overline{\mathfrak{N}}$ ein zu $\{A_2\overline{\mathfrak{N}}\}/\overline{\mathfrak{N}}$ komplementärer direkter Faktor von $\mathfrak{N}_1^*/\overline{\mathfrak{N}}$.

Wir wenden die Kongruenz (K) auf das Element A_2 an. Sind die Repräsentanten P, T innerhalb $\mathfrak{P}_1^*, \mathfrak{G}_1$ gewählt, so gehören die in (K) auftretenden Faktoren $A_2^{PT}, (A_2^{p^r})^{PT}$ sogar zu $\mathfrak{P}_1^* = \mathfrak{P} \cap \mathfrak{G}_1$. Man hat daher wie unter c) Kongruenzen

$$A_2^{PT} \equiv A_2^x, (A_2^{p^r})^{PT} \equiv A_2^y \text{ mod. } \mathfrak{P}_2, \quad \text{also auch mod. } \mathfrak{N}_2.$$

Dabei ist wieder durchweg $y = y_0 p$. Denn wäre $y \not\equiv 0$ mod. p, so hätte das zu $\mathfrak{P}_1^*$ gehörige Element $(A_2^{p^r})^{PT}$ mod. $\mathfrak{P}_2$ und somit erst recht mod. $\overline{\mathfrak{P}}$ die maximale in $\mathfrak{P}_1^*/\overline{\mathfrak{P}}$ vorkommende Ordnung p^{k_2}, während wegen $r \geqq 1$ seine absolute Ordnung niedriger als die von A_2 ist, im Widerspruch zur Wahl von A_2. Hiernach ergibt sich aus (K) wieder eine Kongruenz der Form

$$(V_2) \qquad V(A_2) \equiv A^{1+h_2 p} \text{ mod. } \mathfrak{N}_2$$

mit einem gewissen h_2. Diese besagt analog wie unter d), daß das Element A_2 mod. $\mathfrak{G}_0$ mindestens die Ordnung p^{k_2} hat. Da aber wegen $\mathfrak{G}_1/\mathfrak{G}_0 \cong \mathfrak{P}_1^*/\mathfrak{P}_0$ und $\mathfrak{P}_0^* \geqq \overline{\mathfrak{P}}$ die maximale Ordnung in $\mathfrak{G}_1/\mathfrak{G}_0$ höchstens gleich p^{k_2} ist, folgt wieder wie oben unter d), daß die Untergruppe $\{A_2\mathfrak{G}_0\}/\mathfrak{G}_0$ ein direkter Faktor der Ordnung p^{k_2} von $\mathfrak{G}_1/\mathfrak{G}_0$ ist. Es existiert also ein zu ihr komplementärer direkter Faktor $\mathfrak{G}_2/\mathfrak{G}_0$ derart, daß $\mathfrak{G}_1/\mathfrak{G}_2$ zyklisch von der Ordnung p^{k_2} ist.

Zusammengenommen ist damit die Existenz einer Faktorgruppe $\mathfrak{G}/\mathfrak{G}_2$ vom Typus (p^{k_1}, p^{k_2}) von $\mathfrak{G}/\mathfrak{G}_0$ nachgewiesen.

So fortfahrend gelangt man in m Schritten zu einer Faktorgruppe $\mathfrak{G}/\mathfrak{G}_m$ vom Typus $(p^{k_1}, \ldots, p^{k_m})$ von $\mathfrak{G}/\mathfrak{G}_0$, die also zur vollen Gruppe $\mathfrak{P}/\overline{\mathfrak{P}}$ isomorph ist. Damit ist Satz 9 bewiesen.

Satz 9 liefert insbesondere den bereits in Satz 6 festgestellten Tatbestand. Denn ist speziell $\mathfrak{P}$ abelsch, so ist in Satz 9 $\mathfrak{P}' = 1$, $\overline{\mathfrak{P}} = 1$, also $\overline{\mathfrak{N}} = \overline{\mathfrak{P}}\mathfrak{N}_0 = \mathfrak{N}_0$, und daher $\mathfrak{G}/\mathfrak{G}_0 \cong \mathfrak{N}/\mathfrak{N}_0$.

Um ferner auch den Burnsideschen Satz unter Satz 9 unterzuordnen, beweisen wir noch den folgenden

Zusatz zu Satz 9. *Die in Satz 9 auftretende Gruppe* $\mathfrak{P}_0 = \mathfrak{P} \cap \mathfrak{N}_0$ (*die p-Sylow-*

gruppe der Kommutatorgruppe $\mathfrak{N}'$ des Normalisators $\mathfrak{N}$ von $\mathfrak{P}$) ist auch folgendermaßen charakterisiert:

$\mathfrak{P}_0$ ist der kleinste Normalteiler von $\mathfrak{N}$ derart, daß $\mathfrak{P}/\mathfrak{P}_0$ im Zentrum von $\mathfrak{N}/\mathfrak{P}_0$ liegt.

Beweis. a) $\mathfrak{P}/\mathfrak{P}_0$ liegt wirklich im Zentrum von $\mathfrak{N}/\mathfrak{P}_0$. Denn für P aus $\mathfrak{P}$ und N aus $\mathfrak{N}$ liegt der Kommutator $P^{-1}N^{-1}PN$ einerseits in $\mathfrak{N}'$ und andrerseits in $\mathfrak{P}$, zusammengenommen also in $\mathfrak{P} \cap \mathfrak{N}' = \mathfrak{P}_0$.

b) Sei $\mathfrak{N}^*$ ein Normalteiler von $\mathfrak{N}$, für den $\mathfrak{P}/\mathfrak{N}^*$ im Zentrum von $\mathfrak{N}/\mathfrak{N}^*$ liegt. Nach a) gilt dann dasselbe auch für den Normalteiler $\mathfrak{P}^* = \mathfrak{N}^* \cap \mathfrak{P}_0$ von $\mathfrak{N}$; da danach insbesondere $\mathfrak{P}/\mathfrak{P}^*$ abelsch ist, gilt dabei jedenfalls $\mathfrak{P}^* \geqq \mathfrak{P}'$. Wie oben bei unserem Beweis des Burnsideschen Satzes ergibt sich aus diesem Sachverhalt ohne weiteres

$$V_{\mathfrak{N}\to\mathfrak{P}}(\mathfrak{N}) \equiv V_{\mathfrak{N}\to\mathfrak{P}}(\mathfrak{P}) \equiv \mathfrak{P} \text{ mod. } \mathfrak{P}^*.$$

Daraus folgt in nach dem Bisherigen geläufiger Weise, daß die einerseits zu $\mathfrak{P}/\mathfrak{P}_0$ isomorphe Gruppe $\mathfrak{N}/\mathfrak{N}_0$ andrerseits auch zu $\mathfrak{P}/\mathfrak{P}^*$ isomorph ist. Das besagt aber $\mathfrak{P}^* = \mathfrak{P}_0$, also $\mathfrak{N}^* \geqq \mathfrak{P}_0$. Damit ist der Zusatz bewiesen.

Jetzt wird ersichtlich, wie der Burnsidesche Satz in Satz 9 als Spezialfall enthalten ist. Denn nach dem Zusatz folgt $\mathfrak{P}_0 = 1$, wenn $\mathfrak{P}$ im Zentrum von $\mathfrak{N}$ liegt, und dann liefert Satz 9 die Relation $\mathfrak{G}/\mathfrak{G}_0 \cong \mathfrak{P}/\mathfrak{P}_0 = \mathfrak{P}$.

Die Sätze 1—9 gehören gewissermaßen in einen Zusammenhang. Durch die Sätze 5 bis 9 wird die Frage nach der Ordnung der Kommutatorfaktorgruppe einer Gruppe auf die Frage nach den in den Normalisatoren der Sylowgruppen herrschenden Verhältnissen und den zwischen den konjugierten Sylowgruppen bestehenden Beziehungen zurückgeführt. In den Normalisatoren aber sind die Sylowgruppen Normalteiler, hier können also unter Umständen die Sätze 1—4 Aussagen gestatten.

Eingegangen 2. April 1935.

Über einige Mittelwertfragen im quadratischen Zahlkörper.[1])

Von *L. Rédei* in Göttingen.

Nach einem meiner früheren Sätze [2]) ist die Anzahl der durch 4 teilbaren Invarianten der absoluten Klassengruppe des quadratischen Zahlkörpers allgemein bestimmt. Wie dort, verstehe ich auch hier die Äquivalenz der Ideale im „engeren" Sinne. In dieser Arbeit beschäftige ich mich mit der Frage, wie oft eine beliebige feste Anzahl von durch 4 teilbaren Invarianten zu erwarten ist und wie groß der Mittelwert dieser Anzahl ist. Ich beschränke mich aber auf solche reellen Körper, deren Diskriminante keinen positiven Primzahlteiler der Gestalt $4l + 3$ hat, während ich den allgemeinen Fall später zu betrachten hoffe. In dem ins Auge gefaßten Fall ist bekanntlich die Frage nach dem Vorzeichen der Norm der Grundeinheit unentschieden (sonst ist diese Norm stets positiv). Darauf beziehen sich zwei Sätze [3]), die ich hier kurz Satz$^-$ und Satz$^+$ nenne, welche in gewissen Fällen aus der Diskriminante des Körpers durch Kongruenzbedingungen auf negative bzw. positive Grundeinheitsnorm schließen lassen. Die zweite Aufgabe dieser Arbeit wird es sein, zu prüfen, in welchem Maße diese Sätze anwendbar sind. Auf Grund der Arbeit R werde ich ähnliche Fragen wie die obige auch für die durch 8 teilbaren Invarianten in Angriff nehmen, jedoch ohne so ausführliche Resultate.

Ich bezeichne mit t die Anzahl der verschiedenen Primfaktoren der Diskriminante des Körpers. Meine Untersuchungen werden sich immer auf ein festes, sonst beliebiges t beziehen. Dies wird insofern zweckmäßig sein, als wir einen Überblick haben werden, wie sich die Beantwortung der Fragen für die verschiedenen Werte von t gestaltet. Aus den so erhaltenen Einzelresultaten werden wir aber keine von t freien Aussagen gewinnen können, was seinen Grund letzten Endes darin hat, daß wir keine genügenden Kenntnisse vom Restglied in der Primzahlformel haben.

Wenn a eine unendliche Menge von verschiedenen positiven ganzen Zahlen ist, dann verstehe ich unter $a(x)$ die Anzahl der Elemente aus a, die $\leqq x$ sind, wobei x eine positive Variable ist. Ist dann die Funktion $f(z)$ für die Elemente z der Menge a definiert, so nenne ich

$$\lim_{x\to\infty} \frac{\sum_{z\in a(x)} f(z)}{a(x)}$$

den Mittelwert von $f(z)$ in a oder einfach den Mittelwert von $f(z)$, wenn kein Zweifel vorhanden ist. Ist die Existenz dieses Grenzwertes nicht gesichert, so nenne ich den ent-

[1]) Über dieses Thema habe ich im September 1934 in Bad Pyrmont auf der 10. Jahresversammlung der D. M. V. einen Vortrag gehalten. Diese Arbeit erscheint auch im Math. u. Naturwiss. Anz. d. ung. Ak. in ungarischer Sprache.

[2]) Rédei u. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, dieses Journal **170** (1933), 69—74. Diese Arbeit zitiere ich im folgenden mit RR.

[3]) Rédei, Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, dieses Journal **171** (1934), 131—148. Diese Arbeit zitiere ich im folgenden mit R. — Die genannten Sätze sind unten a. S. 48 formuliert.

sprechenden lim inf und lim sup den unteren bzw. oberen Mittelwert von $f(z)$. Ist b eine Teilmenge von a und ist $f(z)$ so definiert, daß $f(z) = 1$ oder 0 ist, je nachdem z in b liegt oder nicht, so nenne ich den Mittelwert von $f(z)$ die Wahrscheinlichkeit von b (in a), die also nichts anderes als

$$\lim_{x\to\infty} \frac{b(x)}{a(x)}$$

ist. Es ist dann auch klar, was wir unter unterer und oberer Wahrscheinlichkeit zu verstehen haben.

Von den Resultaten dieser Arbeit erwähne ich folgende:

Ich bezeichne stets mit e_2, e_4, e_8 die Anzahl der durch 2, 4 bzw. 8 teilbaren Invarianten der absoluten Klassengruppe eines quadratischen Zahlkörpers. Wenn beliebig gegebene gerade Zahlen vorliegen, dann ist im allgemeinen ungefähr die Hälfte davon durch 4 teilbar. So könnte man erwarten, daß wegen $e_2 = t - 1$ (Gaußscher Satz) e_4 oft ungefähr den Wert $\frac{t-1}{2}$ hat. Dies ist aber bei weitem nicht der Fall. Und zwar hat der Fall $e_4 = 0$ für jedes t eine Wahrscheinlichkeit $> \frac{5}{12}$, und ähnliches gilt auch vom Falle $e_4 = 1$, wenn $t \geqq 6$ ist. Dabei ist die (vereinigte) Wahrscheinlichkeit für $e_4 \leqq 1$ immer $> \frac{5}{6}$. Es kann also $e_4 \geqq 2$ knapp in jedem 6. Falle vorkommen, während z. B. $e_4 \geqq 5$ nicht einmal in jedem 20 000. Falle vorkommt, wie groß auch t sein mag. Trotzdem haben für jedes t die Fälle mit einem festen $e_4 (= 0, 1, 2, \ldots, t-1)$ eine positive Wahrscheinlichkeit, die bei wachsendem e_4 ständig abnimmt. Insbesondere ist die Wahrscheinlichkeit für $e_4 = t - 1$, d. h. dafür, daß jede gerade Invariante in der Klassengruppe zugleich durch 4 teilbar ist, gleich $\frac{1}{2^{\binom{t}{2}}}$.

Als Anwendung wird der Mittelwert von e_4 bei festem t bestimmt. Dieser wächst zwar mit wachsendem t selbst an, doch bleibt er unter einer Grenze 0.764 ... Dieser Mittelwert ist also überraschend klein, wenn wir bedenken, daß $e_2 = t - 1$ mit t ins Unendliche wächst.

Dagegen weist der Mittelwert von e_8 keinen ähnlich starken Rückfall auf. Und zwar übertrifft der untere Mittelwert von e_8 für jedes $t (\geqq 2)$ die Zahl 0.104, höchstens mit Ausnahme von $t = 3$ und 5, aber auch dann liegt dieser untere Mittelwert sicher über 0.093 bzw. 0.102. Dieser verhältnismäßig große Mittelwert von e_8 geht darauf zurück, daß schon der Fall $e_8 = 1$ ziemlich oft vorkommt. Demgegenüber ist die obere Wahrscheinlichkeit für $e_8 = e_2 (= t - 1)$ überaus klein, und zwar $\leqq \frac{1}{2^{t^2-1}}$, was übrigens nach der erwähnten entsprechenden Wahrscheinlichkeitszahl $\frac{1}{2^{\binom{t}{2}}}$ für $e_4 = e_2 (= t - 1)$ zu erwarten war. Dabei sei bemerkt, daß ich die Frage nicht beantworten kann, ob $e_8 = e_2$ für jedes t wirklich vorkommt.

Betreffend die Norm der Grundeinheit bemerke ich zunächst folgendes. Zum Satz$^-$ hat Dirichlet die ersten Beispiele geliefert, indem er die Fälle $t = 2, 3$ untersuchte. Erst hier wird sich (auf arithmetischem Wege) die Tatsache herausstellen, daß die Anwendbarkeit von Satz$^-$ völlig aufhört, sobald $e_4 \geqq 3$. Hierzu ist wegen $e_4 \leqq e_2 = t - 1$ notwendig, daß $t \geqq 4$ ist. Die obigen Fälle $t = 2, 3$ sind also zu einfach, um daraus einen auch nur annähernd guten Einblick in die Frage gewinnen zu können.

Allgemein finden wir, daß bei festem t und $e_4 = e$ (natürlich muß $t > e$ sein) die Wahrscheinlichkeit der Fälle, in denen der Satz$^-$ anwendbar ist, für $e = 0, 1, 2$ und $e \geqq 3$ gleich $1, \frac{1}{4}, \frac{1}{32}$ bzw. 0 ist, wovon das letzte aus der vorigen Bemerkung folgt. Die entsprechende Wahrscheinlichkeit für den Satz$^+$ ist $1 - \frac{1}{2^e}$. Zwar sind diese Wahrscheinlichkeitszahlen formal nur von $e(= e_4)$ abhängig, doch warne ich nochmals davor, diese Resultate als Aussagen zu deuten, die sich auf alle Fälle $e_4 = e$ (ohne eine festgehaltenes t) beziehen. Man sieht, daß für ein großes e_4 die Norm der Grundeinheit überwiegend positiv ist, wie ich es schon in der Arbeit R vermutete. Die Wahrscheinlichkeit der Fälle für festes t und $e_4 = e$, in denen weder der Satz$^-$ noch der Satz$^+$ anwendbar ist, ist also, den Fällen $e = 0, 1, 2, \ldots$ entsprechend, gleich $0, \frac{1}{4}, \frac{7}{32}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \ldots$ Der Fall $e_4 = 1$ ist somit für die Anwendbarkeit dieser Sätze der ungünstigste.

Aus diesen und den vorigen Resultaten, die sich auf e_4 beziehen, erhalten wir dann Aussagen über die Anwendbarkeit dieser beiden Sätze in den Fällen, wo nur t festgehalten wird. Erst diese Feststellungen klären uns über die Tragweite dieser Sätze auf. Davon erwähne ich jetzt nur folgendes: Für jedes feste t ist der Satz$^-$ mit einer Wahrscheinlichkeit > 0.528 anwendbar. Die entsprechende Wahrscheinlichkeit für den Satz$^+$ liegt zwischen $\frac{1}{4}$ und $\frac{1}{3}$, wenn $t \geqq 2$ ist. Der Satz$^-$ ist also wirksamer, obwohl dieser Satz für $e_4 \geqq 3$ nicht anwendbar ist. Dies liegt daran, daß die Fälle $e_4 \leqq 2$ überwiegen. Was uns dann am meisten interessiert, ist, daß für jedes t die Fälle, in denen das Vorzeichen der Norm der Grundeinheit durch den Satz$^-$ und Satz$^+$ nicht entschieden wird, eine Wahrscheinlichkeit < 0.139 haben. Diese Sätze lassen also nicht einmal jeden 7. Fall unbeantwortet.

Aus diesen Resultaten läßt sich ein Überschlag über die Frage machen, in welchem Anzahlverhältnis die Körper zueinander stehen, in denen die Norm der Grundeinheit positiv bzw. negativ ist. Es handelt sich also um die relative Wahrscheinlichkeit der Fälle, in denen diese Norm positiv ist, zu den Fällen, in denen sie negativ ist. Darüber sprach Nagell [4]) auf induktivem Wege die Vermutung aus, daß diese relative Wahrscheinlichkeit (existiert und) ein positiver echter Bruch ist. Unter der Einschränkung, daß wir jedesmal nur die Körper mit einem festen t in Betracht ziehen, läßt sich die Nagellsche Vermutung in dem Sinne bestätigen, sogar verschärfen, daß zwar nicht die Existenz der entsprechenden relativen Wahrscheinlichkeit bewiesen wird, wohl aber sich zwei Funktionen $f_1(t), f_2(t)$ von t so angeben lassen, daß die entsprechenden unteren und oberen relativen Wahrscheinlichkeiten zwischen $f_1(t)$ und $f_2(t)$ liegen. Für jedes $t(\geqq 2)$ gilt hierbei $0 < f_1(t) < f_2(t) < 1$ (während man bekanntlich $f_1(1) = f_2(1) = 0$ annehmen kann) und $\lim f_1(t) = 0.5$, $\lim f_2(t) = 0.891 \ldots$ $(t \to \infty)$, mit einer raschen Konvergenz. Ohne die besagte Einschränkung kann ich jedoch über die Nagellsche Vermutung nichts aussprechen, nur scheint es mir, daß, wenn diese Vermutung richtig ist, der Nagellsche Grenzwert sogar zwischen den eben genannten Zahlen 0.5 und 0.891 ... liegt.

Der I. Teil dieser Arbeit enthält funktionentheoretische Vorbereitungen, im II. und IV. Teil werden die besprochenen Fragen über e_4 und e_8 behandelt, im III. Teile untersuche ich die Frage nach der Norm der Grundeinheit.

I. Teil.

1. R sei der Körper der rationalen Zahlen. Eine ganze Zahl $\mathfrak{p}$ im Körper $R(i)$ $(i^2 = -1)$ nenne ich eine Primzahl in $R(i)$, wenn $(\mathfrak{p})$ ein Primideal ist. Sie heißt eine Primzahl

[4]) Nagell, Über die Lösbarkeit der Gleichung $x^2 - Dy^2 = -1$, Arkiv för Mat., Astr. o. Fysik, **23** B/6 (1932), 1—5.

ersten oder zweiten Grades, wenn ihre Norm $n(\mathfrak{p})$ eine rationale Primzahl oder ein Quadrat davon ist. Primär heißt eine ganze oder gebrochene Zahl α in $R(i)$, wenn $\alpha \equiv 1 \pmod{(1-i)^3}$ ist, wobei die Kongruenz im multiplikativen Sinne aufzufassen ist.

Immer verstehe ich unter $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ solche primären Primzahlen ersten Grades in $R(i)$, für welche $n(\mathfrak{p}_1) < n(\mathfrak{p}_2) < \cdots < n(\mathfrak{p}_t)$ ist. Ferner sei $\mathfrak{P}_t = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_t$.

Ich bezeichne für $t = 1, 2, 3, \ldots$ und $x > 0$ mit $\varkappa_t(x)$ die Anzahl aller Lösungen von $n(\mathfrak{P}_t) \leqq x$.

$\boldsymbol{O}$ und $\boldsymbol{o}$ sind die Landauschen Funktionszeichen. Ist also $f(x)$ eine reelle Funktion, die für hinreichend großes x positiv bleibt und für $x \to \infty$ über alle Grenzen wächst, so sollen $\boldsymbol{O}(f(x))$ und $\boldsymbol{o}(f(x))$ (reelle oder komplexe) Funktionen bedeuten, für die mit wachsendem x $\dfrac{|\boldsymbol{O}(f(x))|}{f(x)}$ unter einer endlichen Schranke bleibt bzw. $\dfrac{\boldsymbol{o}(f(x))}{f(x)}$ gegen 0 konvergiert. Für reelle Funktionen bedeutet $g(x) \sim f(x)$, daß $g(x) = f(x) + \boldsymbol{o}(f(x))$ ist.

Es ist für $t = 1, 2, 3, \ldots$

$$\varkappa_t(x) \sim \frac{1}{(t-1)!} \frac{x(\log\log x)^{t-1}}{\log x}. \tag{1}$$

Davon ist der Fall $t = 1$, d. h. (ich schreibe für $\varkappa_1$ kurz $\varkappa$)

$$\varkappa(x) \sim \frac{x}{\log x}, \tag{2}$$

im wesentlichen die schwächste Form des Primzahlsatzes in $R(i)$. Alle $(\mathfrak{P}_1) = (\mathfrak{p}_1)$ nämlich, deren Anzahl $\varkappa(x)$ ist, sind alle Primideale ersten Grades in $R(i)$ außer $(1-i)$, die eine Norm $\leqq x$ haben. Nun ist (2) richtig, wenn wir zur linken Seite auch die Primideale zweiten Grades mitrechnen, deren Norm $\leqq x$ ist. Diese können aber bekanntlich vernachlässigt werden.

Für $t \geqq 2$ ist (1) eine Formel von Landau [5]). Diese Formel wurde dort (mit π statt $\varkappa$) für den Körper R aufgestellt; der Beweis läßt sich aber wörtlich wiederholen, falls nur immer statt über alle positiven Primzahlen $p \leqq x$ über alle primären Primzahlen ersten Grades in $R(i)$ mit Normen $(n(\mathfrak{p}) =) p \leqq x$ summiert wird. (Diese Normen sind übrigens doppelt so zahlreich wie alle positiven Primzahlen $p \leqq x$ der Gestalt $4l+1$.) Der Landausche Ausgangspunkt [6]) $\vartheta(x) \left(= \sum_{p \leqq x} \log p\right) \sim x$ bleibt nämlich nach dieser Abänderung bestehen.

2. Ich bezeichne das vierte Potenzrestsymbol in $R(i)$ mit $\left(\frac{\alpha}{\beta}\right)_{i4}$ [7]). Sei nun $2 \leqq r \leqq t$, wobei r und t feste ganze rationale Zahlen sind. Ich setze

$$c = \bar{c} \left(\frac{\mathfrak{p}_r}{\mathfrak{a}}\right)_{i4}, \tag{3}$$

wobei $\mathfrak{a}$ ein Potenzprodukt aus den Primzahlen $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_{r-1}$ und den dazu konjugierten, ferner keine vierte Idealpotenz ist, $\bar{c}$ nur von denselben Primzahlen abhängt und $|\bar{c}| = 1$, also auch $|c| = 1$ ist. Dann definiere ich (die komplexwertige Funktion)

$$\varkappa_t(x, c) = \sum_{n(\mathfrak{P}_t) \leqq x} c. \tag{4}$$

Dies ist natürlich so zu verstehen, daß wir in c alle Systeme $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ mit $n(\mathfrak{P}_t) \leqq x$ einsetzen und aus diesen Gliedern die Summe bilden.

---

[5]) Landau, Handbuch der Lehre von der Verteilung der Primzahlen I (1909), 208.

[6]) A. a. O. [5]), 203.

[7]) Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II, Jahresb. d. D. Math. Ver., VI. Ergänzungsbd. (1930), 49—50.

Die analytisch-zahlentheoretische Vorbereitung für die späteren Untersuchungen bildet neben (1) die folgende Formel, deren Beweis allein noch unsere Aufgabe in diesem I. Teil bildet:

$$\varkappa_t(x, c) = \boldsymbol{O}\left(\frac{x(\log\log x)^{t-2}}{\log x}\right) \qquad (t \geqq 2), \tag{5}$$

woraus wegen (1)

$$\lim_{x\to\infty} \frac{\varkappa_t(x, c)}{\varkappa_t(x)} = 0 \qquad (t \geqq 2) \tag{6}$$

folgt.

Es bezeichne p eine positive Primzahl und P_t ein Produkt aus t verschiedenen positiven Primzahlen. Ich beweise zunächst zwei Hilfssätze.

Hilfssatz A. *Es ist für* $t \geqq 1$

$$\sum_{P_t \leqq \frac{x}{10}} \frac{\frac{x}{P_t}}{\log^2 \frac{x}{P_t}} = \boldsymbol{O}\left(\sum_{P_{t-1} \leqq \frac{x}{10}} \frac{\frac{x}{P_{t-1}}}{\log \frac{x}{P_{t-1}}}\right), \tag{7}$$

wobei diese Formel für $t = 1$ *die Form*

$$\sum_{p \leqq \frac{x}{10}} \frac{\frac{x}{p}}{\log^2 \frac{x}{p}} = \boldsymbol{O}\left(\frac{x}{\log x}\right) \tag{8}$$

hat.

Hilfssatz B. *Es ist für* $t \geqq 1$

$$\sum_{P_t \leqq \frac{x}{10}} \frac{\frac{x}{P_t}}{\log \frac{x}{P_t}} = \boldsymbol{O}\left(\frac{x\,(\log\log x)^t}{\log x}\right), \tag{9}$$

insbesondere also für $t = 1$

$$\sum_{p \leqq \frac{x}{10}} \frac{\frac{x}{p}}{\log \frac{x}{p}} = \boldsymbol{O}\left(\frac{x \log\log x}{\log x}\right). \tag{10}$$

Aus (7) und (9) folgt dann

$$\sum_{P_t \leqq \frac{x}{10}} \frac{\frac{x}{P_t}}{\log^2 \frac{x}{P_t}} = \boldsymbol{O}\left(\frac{x\,(\log\log x)^{t-1}}{\log x}\right) \qquad (t \geqq 1). \tag{11}$$

Beweis der Hilfssätze. Ich setze für $2 \leqq u \leqq x$

$$F(u, x) = \frac{\frac{10x}{u}}{\log^2 \frac{10x}{u}} \tag{12}$$

und rechne das Integral

$$\mathfrak{J} = \int_2^x \frac{F(u, x)}{\log u}\, du \tag{13}$$

aus. Es ist

$$\mathfrak{J} = 10x \int_2^x \frac{du}{u \log u \,(\log 10x - \log u)^2} = 10x \int_{\log 2}^{\log x} \frac{dv}{v(a-v)^2},$$

wobei v durch $v = \log u$ als neue Integrationsvariable eingeführt und für den Augenblick $a = \log 10x$ gesetzt wurde. Wegen

$$\frac{1}{v(a-v)^2} = \frac{1}{a^2}\left(\frac{1}{v} + \frac{1}{a-v} + \frac{a}{(a-v)^2}\right)$$

ist dann

$$\mathfrak{J} = \frac{10x}{a^2}\left[\log v - \log(a-v) + \frac{a}{a-v}\right]_{\log 2}^{\log x}$$

$$= \frac{10x}{(\log 10x)^2}\left(\log\log x - \log\log 10 + \frac{\log 10x}{\log 10} - \log\log 2 + \log\log 5x - \frac{\log 10x}{\log 5x}\right).$$

Daraus folgt offenbar

$$\mathfrak{J} = \boldsymbol{O}\left(\frac{x}{\log x}\right). \tag{14}$$

Nunmehr behaupte ich:

1. $F(u, x) \geqq 0$ (für $2 \leqq u \leqq x$).
2. Bei festem $x > 2$ nimmt

$$\frac{F(u, x)}{\log u}$$

von $u = 2$ bis $u = x$ mit wachsendem u niemals zu.

3. $F(2, x) = \boldsymbol{o}\left(\int_2^x \frac{F(u, x)}{\log u} du\right)$.

Davon ist 1. trivial. Statt 2. zeige ich, daß sogar $F(u, x)$ nie zunimmt. $F(u, x)$ hat nämlich vom Faktor $10x$ abgesehen den Wert

$$\frac{1}{u(\log 10x - \log u)^2}.$$

Es genügt also zu zeigen, daß hier der Nenner im Intervalle $2 \leqq u \leqq x$ einen positiven Differentialquotienten nach u hat. In der Tat zerfällt dieser Differentialquotient

$$(\log 10x - \log u)^2 - 2(\log 10x - \log u)$$

in zwei positive Faktoren:

$\log 10x - \log u$ und $\log 10x - \log u - 2 = (\log 10 - \log e^2) + (\log x - \log u)$.

Auch 3. ist richtig, denn die rechte Seite davon ist nach (13) und (14) $\boldsymbol{o}\left(\frac{x}{\log x}\right)$, während die linke Seite wegen (12) $\boldsymbol{O}\left(\frac{x}{\log^2 x}\right)$ ist.

Aus 1. — 3. folgt [6])

$$\sum_{p \leqq x} F(p, x) \sim \int_2^x \frac{F(u, x)}{\log u} du,$$

d. h. nach (13) und (14)

$$\sum_{p \leqq x} F(p, x) = \boldsymbol{O}\left(\frac{x}{\log x}\right).$$

Nach Ersetzen von x durch $\frac{x}{10}$ folgt hieraus wegen (12) die Gleichung (8).

Die linke Seite von (7) läßt sich im Falle $t \geqq 2$ als

$$\sum_{P_{t-1} \leqq \frac{x}{10}} \sum_{p_{t-1} < p \leqq \frac{x}{10 P_{t-1}}} \frac{\frac{x}{p P_{t-1}}}{\log^2 \frac{x}{p P_{t-1}}}$$

schreiben, und die Summe wird höchstens vergrößert, wenn wir die zweite Summe über $2 \leqq p \leqq \frac{x}{10 P_{t-1}}$ erstrecken. Nach Anwendung von (8) auf $\frac{x}{P_{t-1}}$ statt x folgt dann (7), womit der Hilfssatz A bewiesen ist.

Ich benutze das schon erwähnte Landausche Zeichen $\pi_t(x)$. (Es ist also $\pi_t(x)$ die Anzahl der Zahlen $P_t \leqq x$, insbesondere $\pi_1(x) = \pi(x)$ die Anzahl der Primzahlen $p \leqq x$.) Dann gilt [8])

$$\pi_2(x) \sim \frac{1}{2} \sum_{p \leqq x} \pi\left(\frac{x}{p}\right).$$

Wie schon erwähnt, besteht auch für π (statt $\varkappa$) die Relation (1), und somit folgt

$$\sum_{p \leqq x} \pi\left(\frac{x}{p}\right) \sim 2 \frac{x \log\log x}{\log x}.$$

Die linke Seite läßt sich in zwei Teile spalten, indem wir zunächst von 2 bis $\frac{x}{10}$, danach von $\frac{x}{10}$ bis x summieren. Im zweiten Teile ist dann jeder Summand $\leqq p(10) < 10$, während die Anzahl der Glieder $\leqq \pi(x) \sim \frac{x}{\log x}$ ist, so daß dieser Teil vernachlässigt werden kann. Dadurch erhalten wir

$$\sum_{p \leqq \frac{x}{10}} \pi\left(\frac{x}{p}\right) \sim 2 \frac{x \log\log x}{\log x}.$$

Wegen $\pi(x) = \frac{x}{\log x} + \boldsymbol{O}\left(\frac{x}{\log^2 x}\right)$ ist das allgemeine Glied der Summe von der Form

$$\frac{\frac{x}{p}}{\log \frac{x}{p}} + \boldsymbol{O}\left(\frac{\frac{x}{p}}{\log^2 \frac{x}{p}}\right),$$

und somit folgt nach (8) die Gleichung (10).

Die Gleichung (9) beweise ich durch einen Schluß von t auf $t+1$. Dazu setze ich die Richtigkeit von (9) für t voraus ((9) ist ja nach der jetzt bewiesenen Gleichung (10) für $t = 1$ richtig). Die linke Seite von (9) läßt sich für $t+1$ (statt t) so schreiben:

$$\sum_{P_t \leqq \frac{x}{10}} \sum_{p_t < p \leqq \frac{x}{10 P_t}} \frac{\frac{x}{p P_t}}{\log \frac{x}{p P_t}}.$$

Diese Summe wird höchstens vergrößert, wenn schon von $p = 2$ an summiert wird. Dann geht die Summe wegen (10) in

$$\boldsymbol{o}\left(\sum_{P_t \leqq \frac{x}{10}} \frac{\frac{x}{P_t} \log\log \frac{x}{P_t}}{\log \frac{x}{P_t}}\right)$$

[8]) Vgl. Landau, a. a. O. [5]), 205.

über. Dies wird nochmals höchstens vergrößert, wenn wir $\log\log\frac{x}{P_t}$ durch $\log\log x$ ersetzen. Damit ist (9), d. h. der Hilfssatz B, auf Grund der Induktionsvoraussetzung allgemein bewiesen.

Nunmehr will ich (5) beweisen. Ich erhalte alle $\mathfrak{P}_t$ mit $n(\mathfrak{P}_t) \leqq x$, indem ich zunächst nur $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_{r-1}, \mathfrak{p}_{r+1}, \ldots, \mathfrak{p}_r$ nehme, deren Produkt ich mit $\mathfrak{P}$ bezeichne; dann nehme ich $\mathfrak{p}_r$, das ich auch mit $\mathfrak{p}$ bezeichne. Und zwar sollen folgende Bedingungen erfüllt sein:

1. $n(\mathfrak{p}_1) < n(\mathfrak{p}_2) < \cdots < n(\mathfrak{p}_{r-1}) < n(\mathfrak{p}_{r+1}) < \cdots < n(\mathfrak{p}_t), \quad n(\mathfrak{P}) \leqq x,$

2. $$n(\mathfrak{p}_{r-1}) < n(\mathfrak{p}) < n(\mathfrak{p}_{r+1}), \quad n(\mathfrak{p}) \leqq \frac{x}{n(\mathfrak{P})}.$$

Dann kann ich (4) in folgender Form schreiben:

(15) $$\varkappa_t(x, c) = \sum_{n(\mathfrak{P}) \leqq x} \sum_{\substack{n(\mathfrak{p}_{r-1}) < n(\mathfrak{p}) < n(\mathfrak{p}_{r+1}) \\ n(\mathfrak{p}) \leqq \frac{x}{n(\mathfrak{P})}}} c \ ,$$

wobei c so zu verstehen ist, daß wir uns auch in (3) $\mathfrak{p}$ statt $\mathfrak{p}_r$ denken. Wir können die rechte Seite von (15) in zwei Teile spalten, indem wir in der ersten Summe zunächst bis $\frac{x}{10}$, danach von $\frac{x}{10}$ bis x summieren. Im zweiten Teile ist dann $n(\mathfrak{p}) \leqq 10$ und dabei $|c| = 1$. Somit ist dieser Teil $\boldsymbol{O}(\varkappa_{t-1}(x))$, da $\mathfrak{P}$ dem $\mathfrak{P}_{t-1}$ ähnlich definiert ist. Aus (15) und (3) folgt also

(16) $$\varkappa_t(x, c) = \sum_{n(\mathfrak{P}) \leqq \frac{x}{10}} \bar{c}\, S + \boldsymbol{O}(\varkappa_{t-1}(x)) \, ,$$

wobei

(17) $$S = \sum_{\mathfrak{p}} \left(\frac{\mathfrak{p}}{\mathfrak{a}}\right)_{i4}$$

und diese Summe über dieselben $\mathfrak{p}$ zu erstrecken ist wie in (15). Dabei haben wir berücksichtigt, daß c von $\mathfrak{p}$ unabhängig ist.

Ich betrachte jetzt die Strahlklasseneinteilung $\mathfrak{H}_1, \mathfrak{H}_2, \ldots, \mathfrak{H}_f \bmod 4\mathfrak{a}$ aller $\bmod 4\mathfrak{a}$ teilerfremden (ganzen und gebrochenen) Ideale von $R(i)$. Indem ich jedem Primideal ersten Grades aus diesen Klassen eineindeutig diejenige primäre Primzahl $\mathfrak{p}$ in $R(i)$ zuordne, für die durch $(\mathfrak{p})$ das betreffende Ideal hergestellt wird, habe ich eine Beziehung mit allen zu $4\mathfrak{a}$ primen primären Primzahlen ersten Grades von $R(i)$. Wie leicht ersichtlich, erhält man auf diesem Wege in den Summanden von (17) einen Charakter der Strahlklassengruppe. Zunächst enthält nämlich jede Klasse $\mathfrak{H}_k$ ein Primideal ersten Grades, so daß also zu jedem $\mathfrak{H}_k$ ein Charakterwert definiert ist. Sodann ist dieser Wert eindeutig bestimmt. Wenn nämlich $\mathfrak{p}, \mathfrak{p}_0$ zwei zu $4\mathfrak{a}$ prime primäre Primzahlen ersten Grades in $R(i)$ sind und $(\mathfrak{p}), (\mathfrak{p}_0)$ in derselben Klasse $\mathfrak{H}_k$ liegen, so existiert nach der Definition der Strahlklasseneinteilung eine Zahl α in $R(i)$ so, daß

(18) $$(\mathfrak{p}_0) = (\alpha)\,(\mathfrak{p})$$

und

(19) $$\alpha \equiv 1 \pmod{4\mathfrak{a}}$$

ist. Nach dem letzteren ist α primär und auch $\mathfrak{p}, \mathfrak{p}_0$ sind es. Aus (18) folgt also $\mathfrak{p}_0 = \alpha\mathfrak{p}$. Mit Rücksicht auf (19) hängt demnach der Summand in (17) tatsächlich nur von der Klasse $\mathfrak{H}_k$ ab. Daß endlich dieser Wert die erwünschte multiplikative Eigenschaft eines Charakters hat, ist auf Grund der multiplikativen Eigenschaft des Symbols $(-)_{i4}$ analog zu sehen.

Der jetzt betrachtete Charakter ist nicht der Hauptcharakter, da $\mathfrak{a}$ keine vierte Idealpotenz ist. Er ist also von der zweiten oder vierten Ordnung. Bezeichnet daher $n_e (e = 0, 1, 2, 3)$ die Anzahl der Klassen $\mathfrak{H}_k$ mit dem Charakterwert i^e, so ist $n_0 = n_2$, $n_1 = n_3$, wobei eventuell $n_1 = n_3 = 0$ ist. Das S in (17) ist also die Summe von $\frac{f}{2}$ Gliedern der Gestalt $N - N_1$, $i(N - N_1)$, wobei N und N_1 je die Anzahl der Primideale $(\mathfrak{p})$ in irgendeiner Klasse $\mathfrak{H}_k$ bedeuten, die durch die Ungleichungen in (15) beschränkt sind. Nach Landau [9]) ist somit unabhängig von der Klasse $\mathfrak{H}_k$

$$N = \frac{1}{f}\frac{x_1}{\log x_1} + O\left(\frac{x_1}{\log^2 x_1}\right),$$

wobei x_1 als Abkürzung für $\frac{x}{n(\mathfrak{P})}$ gesetzt ist. Daraus folgt dann

$$N - N_1 = O\left(\frac{x_1}{\log^2 x_1}\right).$$

Eine ähnliche Formel gilt also auch für S in (17). Da $|\bar{c}| = 1$, erhalten wir aus (16) die Gleichung

$$\varkappa(x, c) = O\left(\sum_{n(\mathfrak{P}) \leq \frac{x}{10}} \frac{\frac{x}{n(\mathfrak{P})}}{\log^2 \frac{x}{n(\mathfrak{P})}}\right) + O(\varkappa_{t-1}(x)).$$

Hier durchläuft $n(\mathfrak{P})$ alle Produkte $\leqq \frac{x}{10}$ aus $t - 1$ verschiedenen positiven Primzahlen der Gestalt $4l + 1$, jedes davon 2^{t-1}-mal. Da es auf diese Multiplizität nicht ankommt, dürfen wir hier P_{t-1} statt $n(\mathfrak{P})$ schreiben, wobei P_{t-1} wieder die Bedeutung hat wie im Hilfssatze A. Jedenfalls hatten wir hierbei auch die Produkte zugelassen, die nicht nur (positive) Primfaktoren der Gestalt $4l + 1$ haben. Dadurch kann aber diese Beziehung höchstens eine stärkere Gültigkeit erhalten. Auf das erste Glied der rechten Seite können wir dann (11) mit $t - 1$ statt t anwenden, wodurch es in

$$O\left(\frac{x(\log\log x)^{t-2}}{\log x}\right)$$

übergeht. Auch das zweite Glied hat nach (1) einen ähnlichen Wert, womit (5) bewiesen ist.

II. Teil.

3. Ich beweise den folgenden

Hilfssatz C. *Es seien $r(\geqq 0)$ linear unabhängige Linearformen in den Variablen $x_1, x_2, \ldots, x_t$ $(t \geqq 2)$ mit Koeffizienten aus dem Primkörper R_2 der Charakteristik 2 gegeben:*

$$l^m(x) = \sum_{k=1}^{t} c_k^m x_k \qquad (m = 1, 2, \ldots, r). \tag{20}$$

Weiter werde mit den neuen Variablen $x_{ik} (i, k = 1, 2, \ldots, t)$ das folgende System S_t^r von Linearformen gebildet:

$$l_{ik}(x) = x_{ik} + x_{ki} \qquad (1 \leqq i < k \leqq t), \tag{21}$$

$$l_i^m(x) = \sum_{k=1}^{t} c_k^m x_{ik} \quad (i = 1, 2, \ldots, t;\ m = 1, 2, \ldots, r), \tag{22}$$

---

[9]) Landau, Über Ideale und Primideale in Idealklassen, Math. Zeitschr. **2** (1918), 52—154, Satz LXXXV.

so daß also $l_i^m(x)$ *aus* $l^m(x)$ *entsteht, indem* $x_1, x_2, \ldots, x_t$ *durch* $x_{i1}, x_{i2}, \ldots, x_{it}$ *ersetzt werden. Dann ist die Anzahl der linear unabhängigen Formen in* S_t^r, *d. h. der Rang von* S_t^r, *gleich* $t^2 - \binom{t-r+1}{2}$.

Bemerkung. Natürlich sind auch die Formen (21) als Formen von R_2 aufzufassen, indem für die Einheit ε von R_2 immer $\varepsilon x = x$ gesetzt wird. Auch ein leeres Formensystem ist als unabhängig zu betrachten; in diesem Sinne lautet die Behauptung für den Fall $r = 0$ einfach so, daß das System (21) selbst den Rang $t^2 - \binom{t+1}{2} = \binom{t}{2}$ hat.

Offenbar sind die Formen (21) linear unabhängig. Da deren Anzahl $\binom{t}{2}$ ist, ist der Hilfssatz für den Fall $r = 0$ nach der Bemerkung richtig. Ich setze also den Hilfssatz für $r-1$ statt r voraus, um ihn allgemein beweisen zu können.

Ich darf $c_t^r \neq 0$ annehmen, da dies sonst durch geeignete Anordnung von $x_1, x_2, \ldots, x_t$ und von $l^1, l^2, \ldots, l^r$ erreicht werden kann, was die Richtigkeit der Behauptung offenbar nicht beeinflußt. Ferner genügt es, den Fall zu betrachten, in dem alle c_t^m $(m = 1, 2, \ldots, r-1)$ verschwinden. Anderenfalls führe ich die Formen $l'^m(x) = l^m(x) + c_t^m l^r(x)$ $(m = 1, 2, \ldots, r-1)$ ein. Diese Formen zusammen mit $l^r(x)$ $(= l'^r(x))$ sind auch unabhängig, bilden also ebenfalls ein System (20). Dadurch wird ein entsprechendes System $S_t'^r$ definiert, welches aus (21) und aus den Formen

$$\left.\begin{aligned} l_i'^m(x) &= l_i^m(x) + c_t^m l_i^r(x) \quad (m = 1, 2, \ldots, r-1), \\ l'^r(x) &= l_i^r(x) \end{aligned}\right\} \quad (i = 1, 2, \ldots, t)$$

besteht. Ersichtlich hat $S_t'^r$ denselben Rang wie S_t^r, so daß es also genügt, sich für den Beweis auf den obigen Fall zu beschränken.

Es sei also $c_t^1 = c_t^2 = \ldots = c_t^{r-1} = 0$, $c_t^r \neq 0$. Ich führe statt x_{ik} neue Variablen y_{ik} $(i, k = 1, 2, \ldots, t)$ durch die folgende Substitution ein:

$$\begin{aligned} x_{ik} &= y_{ik} && (i, k = 1, 2, \ldots, t-1), \\ x_{it} &= y_{it} + \sum_{k=1}^{t-1} c_k^r y_{ik} && (i = 1, 2, \ldots, t-1), \\ x_{tk} &= y_{tk} + \sum_{i=1}^{t-1} c_i^r y_{ik} && (k = 1, 2, \ldots, t-1), \\ x_{tt} &= y_{tt} + \sum_{k=1}^{t-1} c_k^r (y_{tk} + y_{kk}). \end{aligned}$$

Diese Substitution ist offenbar nicht singulär; daher ist der Rang von S_t^r gleich dem Rang des Systems $S_t'''^r$, das aus S_t^r durch Anwendung dieser Substitution entsteht. Wenn wir berücksichtigen, daß der gemachten Einschränkung wegen die Formen (22) sich auch als

$$\left.\begin{aligned} l_i^m(x) &= \sum_{k=1}^{t-1} c_k^m x_{ik} && (m = 1, 2, \ldots, r-1) \\ l_i^r(x) &= \sum_{k=1}^{t-1} c_k^r x_{ik} + x_{it} \end{aligned}\right\} \quad (i = 1, 2, \ldots, t)$$

schreiben lassen, so ist das System $S_t'''^r$ leicht auszurechnen. Und zwar erhalten wir die folgenden Formen (dabei bedeutet $l_{ik}''(y)$ und $l_i'''^m(y)$ die Form, die durch obige Substitution aus $l_{ik}(x)$ bzw. $l_i^m(x)$ entsteht, während $l_{ik}(y)$, $l_i^m(y)$ die Formen bedeuten, die aus $l_{ik}(x)$ bzw. $l_i^m(x)$ entstehen, wenn einfach x_{uv} überall durch y_{uv} ersetzt wird):

$$l''_{ik}(y) = y_{ik} + y_{ki} = l_{ik}(y) \qquad (1 \leqq i < k \leqq t-1),$$

$$l''_{it}(y) = y_{it} + \sum_{k=1}^{t-1} c_k^r y_{ik} + y_{ti} + \sum_{k=1}^{t-1} c_k^r y_{ki}$$

$$= l_{it}(y) + \sum_{k=1}^{t-1} c_k^r l_{ik}(y) \qquad (i = 1, 2, \ldots, t-1),$$

wobei, falls $i > k$ ist, l_{ki} statt l_{ik} zu setzen ist,

$$l_i''^m(y) = \sum_{k=1}^{t-1} c_k^m y_{ik} = l_i^m(y) \qquad \begin{pmatrix} i = 1, 2, \ldots, t-1 \\ m = 1, 2, \ldots, r-1 \end{pmatrix},$$

$$l_t''^m(y) = \sum_{k=1}^{t-1} c_k^m \left(y_{tk} + \sum_{k=1}^{t-1} c_i^r y_{ik} \right) = l_t^m(y) + \sum_{i=1}^{t-1} c_i^r \sum_{k=1}^{t-1} c_k^m y_{ik}$$

$$= l_t^m(y) + \sum_{i=1}^{t-1} c_i^r l_i^m(y) \qquad (m = 1, 2, \ldots, r-1),$$

$$l_i''^r(y) = \sum_{k=1}^{t-k} c_k^r y_{ik} + y_{it} + \sum_{k=1}^{t-1} c_k^r y_{ik} = y_{it} \qquad (i = 1, 2, \ldots, t-1),$$

$$l_t''^r(y) = \sum_{k=1}^{t-1} c_k^r \left(y_{tk} + \sum_{i=1}^{t-1} c_i^r y_{ik} \right) + y_{tt} + \sum_{k=1}^{t-1} c_k^r (y_{tk} + y_{kk})$$

$$= y_{tt} + \sum_{k=1}^{t-1} \sum_{i=1}^{t-1} c_i^r c_k^r y_{ik} + \sum_{k=1}^{t-1} c_k^r y_{kk}$$

$$= y_{tt} + \sum_{1 \leqq i < k \leqq t-1} c_i^r c_k^r l_{ik}(y),$$

wobei in der letzten Gleichung auch $(c_k^r)^2 = c_k^r$ berücksichtigt wurde.

Wie man leicht sieht, ist dieses System dem folgenden äquivalent:

$l_{ik}(y)$ $(1 \leqq i < k \leqq t)$; $l_i^m(y)$ $(i = 1, 2, \ldots, t;\ m = 1, 2, \ldots, r-1)$; y_{it} $(i = 1, 2, \ldots, t)$.

Von diesem System S ist ein y_{ik} mit $i = t$ oder $k = t$ nur in den Formen des folgenden Teilsystems S_t enthalten:

$l_{ik}(y)$ $(i = 1, 2, \ldots, t-1)$; $l_i^m(y)$ $(m = 1, 2, \ldots, r-1)$; y_{it} $(i = 1, 2, \ldots, t)$.

Umgekehrt enthalten diese Formen nur die eben genannten Variablen. Wenn wir also die übrigen Formen von S mit S_{t-1}^{r-1} bezeichnen, so ist der Rang (von S, d. h.) von S_t^r gleich der Summe des Ranges von S_t und des Ranges von S_{t-1}^{r-1}. Der Rang des ersten ist offenbar $2t-1$, da z. B. die Formen $l_{it}(y)$ $(i = 1, 2, \ldots, t-1)$ und y_{it} $(i = 1, 2, \ldots, t)$ linear unabhängig sind, während die Anzahl der Variablen in S_t auch $2t-1$ ist. Was den Rang von S_{t-1}^{r-1} betrifft, so ist zunächst auch dieses System S_{t-1}^{r-1} ähnlich definiert wie S_t^r, wenn nur $t-1 \geqq 2$, d. h. $t \geqq 3$ ist. Und zwar entsteht S_{t-1}^{r-1} in diesem Falle aus S, wenn

$$t, r, l^m(x) \ (m = 1, 2, \ldots, r) \quad \text{durch} \quad t-1, r-1, l^m(x) \ (m = 1, 2, \ldots, r-1)$$

ersetzt werden (ob wir die Variablen mit x_{ik} oder y_{ik} bezeichnen, macht nichts aus). Dabei ist zu berücksichtigen, daß diese Formen $l^m(x)$ $(m = 1, 2, \ldots, r-1)$ linear unabhängig sind, da sie ein Teilsystem von (20) bilden. Nach der Induktionsvoraussetzung ist also der Rang von S_{t-1}^{r-1} gleich $(t-1)^2 - \binom{t-r+1}{2}$. Addiert man hierzu $2t-1$, so ergibt sich in der Tat $t^2 - \binom{t-r+1}{2}$.

Zum vollständigen Beweis des Hilfssatzes C brauchen wir also nur noch seine Richtigkeit im Ausnahmefalle $t = 2$ zu bestätigen. Dann ist natürlich $r \leqq 2$. Da der Fall $r = 0$ allgemein erledigt ist, brauchen wir nur die Fälle $r = 1, 2$ zu prüfen. Der Fall $r = t$ ist allgemein klar, da die Formen (22) offenbar unabhängig sind und ihre Anzahl rt jetzt gleich t^2 ist. Da dies zugleich die Anzahl der Variablen in S_t^r ist, ist also auch der

Rang t^2 und damit die Behauptung bewiesen. Es bleibt somit nur noch der Fall $t=2, r=1$ übrig. Der behauptete Rang ist in diesem Falle 3, und wir sehen in der Tat, daß die Formen von S_2^1, d. h. $x_{12}+x_{21}, c_1^1 x_{11}+c_2^1 x_{12}, c_1^1 x_{21}+c_2^1 x_{22}$ linear unabhängig sind, da der Fall $c_1^1=c_2^1=0$ nicht vorkommen kann. Damit ist der Hilfssatz C bewiesen.

4. Im folgenden sei D die Diskriminante eines reell-quadratischen Zahlkörpers $R(\sqrt{D})$ ohne positive Primfaktoren der Gestalt $4l+3$. Die Anzahl t der verschiedenen Primfaktoren von D sei fest gewählt. Ich nehme D immer in der Form $D=p_1 p_2 \cdots p_t$ an, wobei $p_1, p_2, \ldots, p_t$ für $2 \nmid D$ positive Primzahlen mit $p_1<p_2<\cdots<p_t$ sind, während für $2 \mid D$ $p_1=8$ ist und $p_2, p_3, \ldots, p_t$ positive Primzahlen mit $p_1<p_2<\cdots<p_t$ sind. Dadurch ist zwischen D und den möglichen Systemen $p_1, p_2, \ldots, p_t$ eine eineindeutige Zuordnung festgelegt. Ich werde später auch eine Funktion (ein Funktionensystem) der Variablen $p_1, p_2, \ldots, p_t$ als Funktion (Funktionensystem) von D betrachten, ohne diese Zuordnung jeweils zu betonen.

Für $t \geqq 2$ nenne ich das System $T=\left(\left(\frac{p_1}{p_2}\right), \left(\frac{p_1}{p_3}\right), \ldots, \left(\frac{p_1}{p_t}\right); \left(\frac{p_2}{p_3}\right), \ldots; \ \ldots, \left(\frac{p_{t-1}}{p_t}\right)\right)$ den quadratischen Typus von D. Für $t=1$ soll der quadratische Typus T von D aus dem einzigen Element 1 bestehen. Die Anzahl der verschiedenen quadratischen Typen ist offenbar $2^{\binom{t}{2}}$, die nach dem quadratischen Reziprozitätsgesetze und dem Satze von der arithmetischen Progression alle möglich sind.

Immer soll $D(x, t)$ die Anzahl der $D \leqq x$ bei festem t bezeichnen. Ähnlich bezeichnet $D(x, T)$ die Anzahl der $D \leqq x$ mit dem quadratischen Typus T. (Statt $D(x, T)$ will ich nicht etwa $D(x, t, T)$ schreiben, weil T schon ein bestimmtes t voraussetzt.) Dann gilt der folgende Satz:

Satz I. *Es ist*

$$D(x,t) \sim \frac{1}{2^t (t-1)!} \frac{x (\log\log x)^{t-1}}{\log x} \tag{23}$$

und unabhängig von T (d. h. nur von t abhängig)

$$\lim_{x\to\infty} \frac{D(x,T)}{D(x,t)} = \frac{1}{2^{\binom{t}{2}}}. \tag{24}$$

Dieser Satz besagt, daß bei jedem festen t unter allen D jeder quadratische Typus T unendlich oft, und zwar mit der gleichen Wahrscheinlichkeit $\frac{1}{2^{\binom{t}{2}}}$ vorkommt.

Beweis. Die Formel (23) ist eine Folgerung aus (1). Nach der Definition ist nämlich die linke Seite von (1) die Anzahl der Lösungen von $n(\mathfrak{P}_t) \leqq x$. Es ist aber $n(\mathfrak{P}_t)$ ein (ungerades) D und jedes ungerade $D \leqq x$ wird auf diesem Wege genau 2^t-mal dargestellt. Die Formel (23) ist also bis auf die geraden D richtig. Die Anzahl der letzteren $D \leqq x$ ist für $t \geqq 2$ offenbar $\leqq \pi_{t-1}\left(\frac{x}{8}\right) \leqq \pi_{t-1}(x)$, wobei wieder das Landausche Zeichen angewendet wurde, d. h. diese Anzahl ist $\boldsymbol{O}\left(\frac{x(\log\log x)^{t-2}}{\log x}\right)$, im Falle $t=1$ sogar nur 1. Die geraden D können also in der Gleichung (23) vernachlässigt werden, womit diese bewiesen ist.

Die Gleichung (24) braucht man nur für $t \geqq 2$ zu beweisen, da sie für $t=1$ nichts aussagt. Dann ist ein quadratischer Typus T durch die Festsetzung $\left(\frac{p_k}{p_l}\right)=a_{kl}$ $(1 \leqq k<l \leqq t)$

gegeben, wobei a_{kl} feste Zahlen ± 1 sind. Setzt man

$$g = \prod_{1 \leqq k < l \leqq t} \frac{1}{2}\left(1 + a_{kl}\left(\frac{p_k}{p_l}\right)\right), \tag{25}$$

so ist offenbar $g = 1$ oder 0, je nachdem D vom quadratischen Typus T ist oder nicht. Es gilt deshalb die Darstellung

$$D(x, T) = \sum_{D \leqq x} g,$$

wobei über alle D mit dem festen t und $\leqq x$ zu summieren ist.

Nach (25) ist also

$$D(x, T) = \frac{1}{2^{\binom{t}{2}}}\left(\sum_{D \leqq x} 1 + \sum_{D \leqq x} \sum_{c} c\right), \tag{26}$$

wobei c ein Produkt aus gewissen verschiedenen der Symbole $\left(\frac{p_k}{p_l}\right)$ $(1 \leqq k < l \leqq t)$ ist, versehen mit einem Vorzeichen, das nur von den a_{kl} abhängt, und c wenigstens ein solches Symbol als Faktor wirklich enthält.

Die erste Summe in (26) ist $D(x, t)$. Zum Beweis von (24) genügt es wegen (23) zu zeigen, daß für jedes c

$$\sum_{D \leqq x} c = \boldsymbol{O}\left(\frac{x\,(\log\log x)^{t-2}}{\log x}\right) \tag{27}$$

ist.

Nun läßt sich c wegen des quadratischen Reziprozitätsgesetzes auf die Form $c = \bar{c}\left(\frac{a}{p_r}\right)$ bringen, wobei $2 \leqq r \leqq t$, a ein nichtleeres Produkt aus gewissen verschiedenen der $p_1, p_2, \ldots, p_{r-1}$ und $\bar{c}$ von $p_r, p_{r+1}, \ldots, p_t$ unabhängig ist. Aus ähnlichen Gründen wie oben brauchen wir in (27) nur die ungeraden D in Betracht zu ziehen. Dann bezeichne ich mit $\mathfrak{p}_k$ $(k = 1, 2, \ldots, t)$ eine primäre Primzahl im Körper $R(i)$, die ein Teiler von p_k ist; es ist also $p_k = \mathfrak{p}_k \mathfrak{p}_k'$, wobei der Strich die konjugierte Zahl in $R(i)$ bezeichnet. Bekanntlich ist

$$\left(\frac{a}{p_r}\right) = \left(\frac{a}{\mathfrak{p}_r}\right)_i,$$

wobei das letztere das zweite Potenzrestsymbol in $R(i)$ ist. Nach dem quadratischen Reziprozitätsgesetze in $R(i)$ und den Grundeigenschaften der Potenzrestsymbole ist weiter

$$\left(\frac{a}{p_r}\right) = \left(\frac{\mathfrak{p}_r}{a}\right)_i = \left(\frac{\mathfrak{p}_r}{a^2}\right)_{i4}.$$

Da a^2 ein Produkt aus einigen der $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_{r-1}, \mathfrak{p}_1', \ldots, \mathfrak{p}_{r-1}'$ und nach dem obigen keine vierte Idealpotenz in $R(i)$ ist, und auch $\bar{c}$ nur von diesen Primzahlen abhängt, endlich $|\bar{c}| = 1$ ist, sehen wir, daß c genau der Definition (3) entspricht. Wir denken uns dieses c in (4) eingesetzt. Dann ist $\varkappa_t(x, c)$ genau das 2^t-fache der linken Seite von (27), wenn wir hierin, wie gesagt, nur die ungeraden D berücksichtigen. Wie schon erwähnt, läßt sich nämlich jedes solche D genau 2^t-mal als Norm von $\mathfrak{P}_t = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_t$ darstellen, entsprechend der freien Wahl zwischen den konjugierten $\mathfrak{p}_k, \mathfrak{p}_k'$ $(k = 1, 2, \ldots, t)$. Unser jetziges c hängt aber von dieser Wahl nicht ab. Somit folgt (27) aus (5), womit der Satz I bewiesen ist.

(Bei diesem Beweis hätten wir einfacher mit einer Formel auskommen können, die (5) ähnlich ist, doch nicht in $R(i)$ mit $(—)_{i4}$, sondern in R mit $(—)$ aufgestellt wäre. Im vollen Umfange wird (5) erst im III. und IV. Teil gebraucht.)

5. Der eingangs erwähnte Satz der Arbeit RR läßt sich für die jetzt betrachteten Körper etwas leichter formulieren.

Indem ich D wieder wie in **4.** in der Form $D = p_1 p_2 \cdots p_t$ annehme, verstehe ich unter einer D-Zerfällung ein Zahlenpaar D', D'', wobei $D'D'' = D$ und D' ein Produkt von verschiedenen der $p_1, p_2, \ldots, p_t$ ist, den Fall $D' = 1$ mitgerechnet. Wenn überdies D' ein quadratischer Rest von D'' und D'' ein quadratischer Rest von D' ist, dann nenne ich D', D'' eine D-Zerfällung zweiter Art.

Wenn D', D'' und D_0', D_0'' zwei D-Zerfällungen sind, dann nenne ich die D-Zerfällung, die aus $D'D_0', D''D_0'$ durch Weglassung sämtlicher Faktoren p_k^2 entsteht, die zusammengesetzte D-Zerfällung. Nach dieser Regel bilden die D-Zerfällungen eine abelsche Gruppe G vom Typus $(2, 2, \ldots, 2)$ und der Ordnung 2^t, mit dem Einheitselement $1, D$. Wie man leicht nachrechnet bilden darin die D-Zerfällungen zweiter Art eine Untergruppe G_2.

Indem ich wieder die Anzahl der durch 4 teilbaren Invarianten der absoluten Klassengruppe des Körpers $R(\sqrt{D})$ mit e_4 bezeichne, lautet der Satz jetzt so: *Bezeichnet r die Anzahl der unabhängigen Elemente in der Gruppe G_2, so ist* $e_4 = r - 1$. (Diese Fassung ist etwas anders als in der Arbeit RR, wo nämlich D', D'' und D'', D' als nicht verschiedene D-Zerfällungen betrachtet wurden, so daß im jetzigen Sinne sowohl G als auch G_2 doppelt so viel Elemente haben.) Anders gesagt, es ist

$$2^{e_4+1} = (G_2), \tag{28}$$

wobei die Klammern die Gruppenordnung bedeuten.

Nach der getroffenen Vereinbarung läßt sich eine D-Zerfällung D', D'' als eine Funktion (genauer gesagt ein Funktionenpaar) von D auffassen, und zwar folgendermaßen. Eine D-Zerfällung D', D'' ist durch $D' = p_{k_1} \cdots p_{k_m}$, $D'' = p_{l_1} \cdots p_{l_n}$ gegeben, wobei die Indizes $k_1, \ldots, k_m$ und $l_1, \ldots, l_n$ zwei komplementäre Teilmengen von $1, 2, \ldots, t$ bilden. Indem wir diese Indizesreihen festhalten, können wir *diese* D', D'' als (eindeutige) Funktionen von D betrachten. Bei dieser Auffassung bleibt eine Gleichung $\Delta_1\Delta_2 = \Delta_3$ unter den D-Zerfällungen $\Delta_1, \Delta_2, \Delta_3$ für alle D aufrecht erhalten. Ähnlich sind also die Begriffe Untergruppe und unabhängige Basis von G gegenüber der besonderen Wahl von D bis auf die metrischen Eigenschaften invariante Gebilde. Wenn wir uns dabei auf die D von einem festen quadratischen Typus T beschränken, so ist auch die Eigenschaft, von zweiter Art zu sein, eine innerhalb dieser D invariante Eigenschaft der betreffenden D-Zerfällung (d. h. die aus einer festen D-Zerfällung für die sämtlichen D desselben quadratischen Typus T entsprungenen D-Zerfälluungen sind entweder alle von der zweiten Art oder sind es alle nicht). In diesem Sinne ist auch die Gruppe G_2 aller D-Zerfällungen zweiter Art (samt der Gruppeneigenschaften) durch T allein bestimmt, insbesondere sind also die Ordnung (G_2) und wegen (28) auch e_4 Funktionen von T allein. (Das hier auseinandergesetzte Prinzip tritt später fast immer auf, wenn es sich um mehrere D zugleich handelt.)

6. Ich bezeichne mit $D(x, t, e)$ die Anzahl der $D \leqq x$, für die t fest ist und überdies e_4 gleich einem festen e $(= 0, 1, \ldots, t-1)$ ist. Ich setze

$$t_e = \lim_{x\to\infty} \frac{D(x, t, e)}{D(x, t)}. \tag{29}$$

Dann ist t_e die Wahrscheinlichkeit der Fälle mit genau e durch 4 teilbaren Invarianten

in der absoluten Klassengruppe unter allen Körpern $R(\sqrt{D})$, deren Diskriminante aus t verschiedenen Primzahlfaktoren zusammengesetzt ist.

Der Zähler in (29) ist die Summe derjenigen $D(x, T)$, in welchen $e_4 = e$ für T ist, und somit folgt aus dem Satz I:

$$t_e = \frac{\textit{Anzahl der } T \textit{ mit } e_4 = e}{2^{\binom{t}{2}}} \qquad (0 \leqq e \leqq t-1). \tag{30}$$

7. Um t_e zu ermitteln, setze ich im folgenden $t \geqq 2$ voraus.

Ich nehme ein beliebiges $D = p_1 p_2 \cdots p_t$ an. Dann setze ich

$$\left(\frac{p_i}{p_k}\right) = (-1)^{x_{ik}} \qquad (i, k = 1, 2, \ldots, t;\ i \neq k) \tag{31}$$

und definiere noch x_{ii} $(i = 1, 2, \ldots, t)$ durch

$$\sum_{k=1}^{t} x_{ik} \equiv 0 \pmod 2. \tag{32}$$

Dabei sollen alle x_{ik} $(i, k = 1, 2, \ldots, t)$ gleich 0 oder 1 sein. Wegen (31) ist

$$x_{ik} + x_{ki} \equiv 0 \pmod 2 \qquad (1 \leqq i < k \leqq t). \tag{33}$$

Nun wähle ich eine beliebige D-Zerfällung D', D'' und setze mit $c_i = 0, 1$

$$D' = p_1^{c_1} p_2^{c_2} \cdots p_t^{c_t}. \tag{34}$$

Dann ist

$$D'' = p_1^{1-c_1} p_2^{1-c_2} \cdots p_t^{1-c_t}. \tag{35}$$

Ich definiere noch die Linearform

$$l(x) \equiv \sum_{k=1}^{t} c_k x_k \pmod 2. \tag{36}$$

Offenbar ist $l(x)$ der D-Zerfällung D', D'' eindeutig zugeordnet. Nun behaupte ich folgendes:

Dann und nur dann ist die D-Zerfällung D', D'' von der zweiten Art, wenn für die in (36) *zugeordnete Linearform $l(x)$ nach Einsetzen der durch* (31) *und* (32) *definierten Zahlen $x_{i1}, x_{i2}, \ldots, x_{it}$ statt $x_1, x_2, \ldots, x_t$*

$$l_i(x) \equiv \sum_{k=1}^{t} c_k x_{ik} \equiv 0 \pmod 2 \qquad (i = 1, 2, \ldots, t) \tag{37}$$

ist.

Zunächst betrachten wir die D-Zerfällungen $1, D$ und $D, 1$. Beide sind nach der Definition von der zweiten Art. Andererseits sind die in (36) zugeordneten Formen $l(x) \equiv 0$ bzw. $\sum_{k=1}^{t} x_i \pmod 2$, für welche (37) trivialerweise bzw. wegen (32) erfüllt ist.

Dann betrachte ich eine beliebige D-Zerfällung D', D'' mit $1 < D' < D$. Nach der Definition ist diese dann und nur dann von der zweiten Art, wenn für jeden Faktor p_i von D''

$$\left(\frac{D'}{p_i}\right) = 1 \qquad (p_i \mid D'') \tag{38}$$

und für jeden Faktor p_i von D'

$$\left(\frac{D''}{p_i}\right) = 1 \qquad (p_i \mid D') \tag{39}$$

ist.

Die Gleichung (38) läßt sich auch in der Form $\left(\frac{p_i}{D'}\right) = 1$ schreiben. Dann ist die linke Seite nach (34) und (31)

$$\left(\frac{p_i}{D'}\right) = \prod_{k=1}^{t}\left(\frac{p_i}{p_k}\right)^{c_k} = (-1)^{\sum_{k=1}^{t} c_k x_{ik}}.$$

Das Bestehen von (38) bedeutet, daß dieser Exponent gerade ist, d. h. daß (37) für alle Indizes i richtig ist, für die $p_i \mid D''$. Ähnlich schreibe ich (39) in der Form $\left(\frac{p_i}{D''}\right) = 1$. Dann läßt die linke Seite auf Grund von (35) und (31) eine ähnliche Umformung zu wie früher, wobei jetzt der Exponent

$$\sum_{k=1}^{t}(1 - c_k)\, x_{ik}$$

auftritt. Dieser Exponent geht aber mod 2 wegen (32) in den vorigen über. (39) ist also nichts anderes als die Bedingung dafür, daß (37) für die *übrigen* Indizes i gilt, für die nämlich $p_i \mid D'$ ist. Damit ist die Behauptung bewiesen.

Wir beweisen den folgenden

Hilfssatz D. *Ist G^r eine Untergruppe der Gruppe G aller D-Zerfällungen, die die Ordnung 2^r hat und das Element $D, 1$ enthält, so ist*

$$2^{\binom{t-r+1}{2}}$$

die Anzahl derjenigen quadratischen Typen T, für die die Gruppe G^r aus lauter D-Zerfällungen zweiter Art besteht.

Bezeichne nämlich Δ eine beliebige D-Zerfällung und $l(x)$ die ihr durch (34) und (36) zugeordnete Linearform mod 2. Offenbar ist kraft dieser Zuordnung die Gruppe G aller Δ (einstufig) isomorph mit der additiven Gruppe g aller solchen Linearformen $l(x)$ (mod 2), die (36) ähnlich sind. In dieser Isomorphie entspricht der Untergruppe G^r eine Untergruppe g^r von g. Sei nun $\Delta_1, \Delta_2, \ldots, \Delta_r$ eine unabhängige Basis für G^r, der dann auch eine unabhängige Basis $l^1(x), l^2(x), \ldots, l^r(x)$ von g^r entspricht. Aus dem über (37) Bewiesenen folgt offenbar, daß G^r dann und nur dann aus lauter D-Zerfällungen zweiter Art besteht (wenn auch $\Delta_1, \Delta_2, \ldots, \Delta_r$ von der zweiten Art sind, d. h.) wenn für alle Formen $l^1(x), l^2(x), \ldots, l^r(x)$ die zu (37) analogen Kongruenzen

$$l_i^m(x) \equiv 0 \pmod 2 \quad (m = 1, 2, \ldots, r;\ i = 1, 2, \ldots, t) \tag{40}$$

erfüllt sind (auch hier bedeutet der Index i das Einsetzen der Werte $x_{i1}, x_{i2}, \ldots, x_{it}$ aus (31), (32) an Stelle von $x_1, x_2, \ldots, x_t$). Da G^r nach Voraussetzung die D-Zerfällung $D, 1$ enthält, können wir z. B. $\Delta_1 = D, 1$ annehmen, was dann, wie schon erwähnt, bedeutet, daß

$$l^1(x) \equiv \sum_{k=1}^{t} x_k \pmod 2$$

ist.

Wir können also folgendes sagen: Um alle quadratischen Typen T zu finden, für die G^r aus lauter D-Zerfällungen zweiter Art besteht, sind die Symbole $\left(\frac{p_i}{p_k}\right)(1 \leqq i < k \leqq t)$, d. h. wegen der Zuordnung in (31) die Zahlen $x_{ik}(= 0, 1)$ für $1 \leqq i < k \leqq t$, auf alle möglichen Arten so zu bestimmen, daß diese Zahlen zusammen mit den durch sie nach (33), (32) bestimmten Zahlen x_{ik} $(1 \leqq k \leqq i \leqq t)$ die Kongruenzen (40) befriedigen. Die Anzahl dieser T ist also die Anzahl der Lösungen des Kongruenzensystems (32), (33), (40). Von dem System (40) sind aber die Kongruenzen mit $m = 1$ wegen der Annahme über $l^1(x)$ nichts anderes als die Kongruenzen (32). Man hat also einfach die Kongruenzen (33), (40) zu lösen. Da die Kongruenzklassen (mod 2) den Prim-

körper R_2 bilden, folgt aus dem Hilfssatz C, daß der Rang der Linearformen (mod 2) auf den linken Seiten dieser Kongruenzen gleich $t^2 - \binom{t-r+1}{2}$ ist. Die Anzahl der Unbekannten ist t^2. Somit lassen sich bei der Lösung genau $\binom{t-r+1}{2}$ Unbekannte beliebig wählen. Da hierfür nur die Werte 0, 1 in Betracht kommen, folgt die Richtigkeit des Hilfssatzes D.

8. Ich bezeichne mit $\{t, G^r\}$ die Anzahl der quadratischen Typen T, für die die Gruppe der D-Zerfällungen zweiter Art gleich G^r ist. Da $D, 1$ eine D-Zerfällung zweiter Art ist, hat diese Definition nur einen Sinn, wenn $D, 1$ in G^r enthalten ist. Dies wollen wir also voraussetzen. Sonst soll G^r eine beliebige Untergruppe von G bedeuten, und in dieser Bezeichnung soll immer 2^r die Ordnung von G^r sein.

Wir wollen unter dieser Voraussetzung den Wert von $\{t, G^r\}$ ermitteln. Zunächst gilt die folgende Formel:

$$2^{\binom{t-r+1}{2}} = \sum_{G^r \leq G^s \leq G} \{t, G^s\}, \tag{41}$$

wobei in der Summe G^s alle Gruppen zwischen der festen Untergruppe G^r und der Gruppe G durchläuft.

Diese Formel entsteht folgendermaßen: Wir betrachten alle quadratischen Typen T, für die die Gruppe aller D-Zerfällungen zweiter Art eine Gruppe G^s ist, wobei G^s den entsprechenden Bedingungen genügt wie in (41). Die Anzahl dieser T ist der Summand in (41). Indem wir G^s zwischen G^r und G variieren lassen, sind die betrachteten T genau die, für die die feste Gruppe G^r aus lauter D-Zerfällungen zweiter Art besteht, jedes T einmal gerechnet. Da deren Anzahl nach dem Hilfssatz D gleich der linken Seite von (41) ist, ist die Richtigkeit dieser Formel bestätigt.

Ich behaupte nun die allgemeine Formel:

$$\{t, G^r\} = \{t - r\}, \tag{42}$$

wobei

$$\{0\} = \{1\} = 1, \quad \{l\} = (2^1 - 1)(2^2 - 1)\cdots(2^l - 1)\frac{2^2 \cdot 2^4 \cdots 2^{2\left[\frac{l}{2}\right]}}{(2^2 - 1)(2^4 - 1)\cdots(2^{2\left[\frac{l}{2}\right]} - 1)} \tag{43}$$

$$(l = 2, 3, \ldots)$$

und $[z]$ für reelle Zahlen z die größte ganze Zahl $\leqq z$ bedeutet. (Insbesondere hängt also $\{t, G^r\}$ nur von $t - r$ ab.)

Es ist zunächst sofort zu sehen, daß durch (41) alle $\{t, G^r\}$ eindeutig bestimmt sind. Für ein festes t ergibt nämlich (41), auf den Fall $r = t$, d. h. $G^r = G^t = G$ angewandt, die Beziehung $\{t, G^t\} = 1$. Für den Fall $r = t - 1$ folgt weiter

$$2 = \{t, G^{t-1}\} + \{t, G^t\}, \quad \text{also} \quad \{t, G^{t-1}\} = 1,$$

wobei G^{t-1} eine beliebige Gruppe der Ordnung 2^{t-1} in G ist, die $D, 1$ enthält. Dann läßt sich $\{t, G^{t-2}\}$ ausrechnen, und so weiter allgemein $\{t, G^r\}$ $(r = t - 3, t - 4, \ldots, 1)$, wenn man berücksichtigt, daß es auf der rechten Seite von (41) nur ein einziges Glied gibt, in dem $s = r$, während in den übrigen Gliedern $s > r$ ist.

Wir haben also (42) bestätigt, wenn wir zeigen, daß alle Gleichungen (41) durch (42) befriedigt werden. Wir setzen demgemäß (42) in (41) ein und zeigen, daß die so erhaltene Gleichung richtig ist.

Bekanntlich ist

$$(44)\qquad \frac{(2^k-1)(2^{k-1}-1)\cdots(2^{k-l+1}-1)}{(2^1-1)(2^2-1)\cdots(2^l-1)}$$

für $k=t-r$ und $l=t-s$ die Anzahl der Untergruppen der Ordnung 2^s in einer abelschen Gruppe der Ordnung 2^t vom Typus $(2, 2, \ldots, 2)$, die eine feste Untergruppe der Ordnung 2^r enthalten (im Falle $l=0$, d. h. $s=t$ ist darunter 1 zu verstehen.).

Wir denken uns (42) in (41) eingesetzt und fassen alle Glieder von (41) zusammen, die zu einem festen s gehören. Da diese alle gleich $\{t-s\}$ sind und ihre Anzahl (44) ist (natürlich mit $k=t-r$, $l=t-s$), haben wir diese beiden Zahlen zu multiplizieren, sodann dieses Produkt für $s=r, r+1, \ldots, t$ zu addieren und endlich zu zeigen, daß diese Summe gleich der linken Seite von (41) ist. Nun sind die Faktoren dieses Produkts gleich der rechten Seite von (43) mit $l=t-s$ und, wie schon gesagt, (44) mit $k=t-r$, $l=t-s$. Somit ist dieses Produkt

$$(45)\quad a_{kl}=(2^k-1)(2^{k-1}-1)\cdots(2^{k-l+1}-1)\,\frac{2^2\cdot 2^4\cdots 2^{2\left[\frac{l}{2}\right]}}{(2^2-1)(2^4-1)\cdots(2^{2\left[\frac{l}{2}\right]}-1)},$$

worunter, falls $l=0$ oder 1 ist, $a_{k0}=1$ und $a_{k1}=2^k-1$ zu verstehen ist. Dies ist also über $s=r, r+1, \ldots, t$, d. h. über $(t-s=)\,l=0, 1, \ldots, k(=t-r)$ zu summieren. Die linke Seite von (41) läßt sich als $2^{\binom{k+1}{2}}$ schreiben. Es lautet also die zu beweisende Gleichung

$$(46)\qquad 2^{\binom{k+1}{2}}=2^k+\sum_{l=2}^{k}a_{kl},$$

wo wir statt $a_{k0}+a_{k1}$ schon 2^k geschrieben haben. Natürlich ist hier die rechte Seite in den Fällen $k=0$ und 1 durch a_{00} bzw. $a_{10}+a_{11}$, d. h. durch 1 bzw. 2 zu ersetzen, da $a_{00}=a_{10}=a_{11}=1$ ist. Man sieht unmittelbar, daß (46) für $k=0$ und 1 richtig ist. Ich setze die Richtigkeit bis $k-1$ voraus und beweise so (46) allgemein.

Für $k=2$ ist (46) richtig, da a_{22} nach (45) gleich 4 ist. Im folgenden dürfen wir also $k\geqq 3$ annehmen.

Wir bemerken auf Grund von (45) zunächst folgendes:

$$(47)\qquad a_{kl}=\frac{2^k-1}{2^{k-l}-1}\,a_{k-1,l} \qquad (k>l\geqq 2),$$

$$(48)\qquad a_{kl}=(2^{k-l+1}-1)\,a_{k,l-1} \qquad (2\nmid l;\ k\geqq l\geqq 3),$$

$$(48\text{a})\qquad a_{kl}=(2^{k-l+1}-1)\,\frac{2^l}{2^l-1}\,a_{k,l-1} \qquad (2\mid l;\ k\geqq l\geqq 4),$$

$$(49)\qquad a_{kk}=2^k a_{k-1,k-1} \qquad (2\mid k;\ k\geqq 4).$$

Sodann zeigen wir die Richtigkeit der folgenden Gleichung:

$$(50)\qquad a_{kl}+a_{k,l+1}=2^k(a_{k-1,l-1}+a_{k-1,l}) \qquad (2\mid l;\ k>l\geqq 2).$$

Nach (48) ist nämlich $a_{k,l+1}=(2^{k-l}-1)a_{kl}$, woraus folgt, daß die linke Seite von (50) gleich $2^{k-l}a_{kl}$ ist. Dann geht (50) in

$$a_{kl}=2^l(a_{k-1,l-1}+a_{k-1,l})$$

über. Nach Anwendung von (47) auf die linke Seite folgt daraus

$$(2^k-1)\,a_{k-1,l}=(2^k-2^l)(a_{k-1,l-1}+a_{k-1,l}).$$

Dies läßt sich in der Form

$$(2^l-1)\,a_{k-1,l}=2^l(2^{k-l}-1)\,a_{k-1,l-1}$$

schreiben. Offenbar folgt umgekehrt die Richtigkeit von (50), wenn diese Gleichung richtig ist. Letzteres ist eine unmittelbare Folgerung aus (48a) (angewandt auf $k-1$ statt k), wenn $l \geqq 4$ ist, während es im restlichen Falle $l = 2$ aus

$$a_{k-1,2} = (2^{k-1}-1)(2^{k-1}-1)\frac{2^2}{2^2-1} \quad \text{und} \quad a_{k-1,1} = 2^{k-1}-1$$

folgt. Damit haben wir (50) bewiesen.

Nunmehr beweisen wir (46). Dabei unterscheiden wir zwei Fälle:

1) $2 \nmid k$ $(k \geqq 3)$. Wir rechnen die Summe auf der rechten Seite von (46) nach dem Schema $(a_{k2}+a_{k3})+(a_{k4}+a_{k5})+\cdots+(a_{k,k-1}+a_{kk})$ aus. Auf jeden Klammerausdruck läßt sich (50) anwenden, wodurch diese Summe in

$$2^k \sum_{l=1}^{k-1} a_{k-1,l} = 2^k\left((2^{k-1}-1)+\sum_{l=2}^{k-1} a_{k-1,l}\right)$$

übergeht. Wenn wir dies in (46) einsetzen und durch 2^k dividieren, erhalten wir eine Gleichung, die nichts anderes ist als die Gleichung (46) für $k-1$ (statt k). Offenbar ist also der Voraussetzung wegen auch (46) richtig.

2) $2 \mid k$ $(k \geqq 4)$. Nun schreiben wir die Summe in (46) so:

$$(a_{k2}+a_{k3})+\cdots(a_{k,k-2}+a_{k,k-1})+a_{kk}.$$

Mit den Klammerausdrücken verfahren wir ähnlich wie oben. Auf das letzte Glied wenden wir (49) an. Verfährt man analog weiter, so erhält man auch in diesem Falle das vorige Resultat.

Damit haben wir (46) und somit (42) bewiesen.

9. Wir sind nunmehr in der Lage, die Wahrscheinlichkeit t_e in (29) zu bestimmen. Dazu brauchen wir nach (30) die Anzahl der quadratischen Typen T, für die $e_4 = e$, wobei e eine feste Zahl von $0, 1, 2, \ldots, t-1$ ist. Nach (28) sind diese Typen diejenigen, für die die Gruppe aller D-Zerfällungen zweiter Art eine Untergruppe G^{e+1} von G ist, wobei G^{e+1} wieder, wie in **8**, von der Ordnung 2^{e+1} ist und die D-Zerfällung $D, 1$ enthält (wie schon öfter erwähnt, i t $D, 1$ immer eine D-Zerfällung zweiter Art). Nun ist die Anzahl der T, zu denen in diesem Sinne ein bestimmtes G^{e+1} gehört, nach (42) gleich $\{t-e-1\}$, d. h. die rechte Seite von (43) mit $l = t-e-1$ und die Anzahl der in Frage kommenden G^{e+1} ist durch (44) mit $r = 1$, $s = e+1$, d. h. mit $k = t-1$, $l = t-e-1$ gegeben (es handelt sich nämlich bei dieser Anzahl um alle Gruppen G^{e+1} der Ordnung 2^{e+1}, die zwischen der Gruppe aus den beiden Elementen $1, D$; $D, 1$ und der Gruppe G liegen). Das Produkt aus diesen beiden Ausdrücke ist also die gesuchte Anzahl der T. Dieses Produkt hatten wir in (45) schon einmal gebildet; hierin ist also jetzt $k = t-1$, $l = t-e-1$ einzusetzen. Dieser Ausdruck $a_{t-1,t-e-1}$ in (45), der nach der dortigen Bemerkung in den Fällen $e = t-2$ und $t-1$ durch $a_{t-1,1} = 2^{t-1}-1$ bzw. $a_{t-1,0} = 1$ zu ersetzen ist, liefert nach (30) durch $2^{\binom{t}{2}}$ dividiert die Zahl t_e. Nach leichter Umformung haben wir somit den folgenden

Satz II. *Unter allen reell-quadratischen Körpern, deren Diskriminante aus t verschiedenen positiven Primzahlen $\not\equiv 3 \pmod 4$ zusammengesetzt ist, haben die Körper mit genau e durch 4 teilbaren Invarianten in der absoluten Klassengruppe eine (positive) Wahrscheinlichkeit*

$$(51) \qquad t_e = \frac{1}{2^{\binom{e+1}{2}}} \frac{\left(1-\frac{1}{2^{t-1}}\right)\left(1-\frac{1}{2^{t-2}}\right)\cdots\left(1-\frac{1}{2^{e+1}}\right)}{\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{2^4}\right)\cdots\left(1-\frac{1}{2^{2\left[\frac{t-e-1}{2}\right]}}\right)} \qquad (0 \leqq e \leqq t-1).$$

In den Fällen $e = t-2$ *und* $t-1$ *ist darunter*

$$t_{t-2} = \frac{1 - \frac{1}{2^{t-1}}}{2^{\binom{t-1}{2}}}, \qquad t_{t-1} = \frac{1}{2^{\binom{t}{2}}} \tag{51a}$$

zu verstehen. (Auch in diesen Fällen ist (51) richtig, wenn wir verabreden, den Zähler und Nenner des zweiten Faktors in (51) durch 1 zu ersetzen, falls sie sonst keinen Sinn haben. Wir haben (51) nur für den Fall $t \geqq 2$ abgeleitet, doch ist es nach dieser Verabredung auch im Falle $t = 1$ richtig, da dann nämlich nur $e = 0$ in Frage kommt, was offenbar den Wert $t_e = 1_0 = 1$ ergibt.)

Wir werden jetzt die eben erhaltenen Wahrscheinlichkeitszahlen t_e nach ihrer Größe untersuchen. Es wird zunächst lehrreich sein, einige Anfangswerte von t_e in einer Tabelle zusammenzustellen:

	$e=$ 0	1	2	3	4	5 ...
$=1$	(1) 1					
2	$\left(\frac{1}{2}\right)$ 0.5	$\left(\frac{1}{2}\right)$ 0.5				
3	$\left(\frac{1}{2}\right)$ 0.5	$\left(\frac{3}{8}\right)$ 0.375	$\left(\frac{1}{8}\right)$ 0.125			
4	$\left(\frac{7}{16}\right)$ 0.4375	$\left(\frac{7}{16}\right)$ 0.4375	$\left(\frac{7}{64}\right)$ 0.1093 ...	$\left(\frac{1}{64}\right)$ 0.0156 ...		
5	$\left(\frac{7}{16}\right)$ 0.4375	$\left(\frac{105}{256}\right)$ 0.4101 ...	$\left(\frac{35}{256}\right)$ 0.1367 ...	$\left(\frac{15}{1024}\right)$ 0.0146 ...	$\left(\frac{1}{1024}\right)$ 0.0009 ...	
6	$\left(\frac{217}{512}\right)$ 0.4236 ...	$\left(\frac{217}{512}\right)$ 0.4236 ...	$\left(\frac{1085}{8192}\right)$ 0.1324 ...	$\left(\frac{155}{8192}\right)$ 0.0189 ...	$\left(\frac{31}{32768}\right)$ 0.0009 ...	$\left(\frac{1}{32768}\right)$ 0.00003 ...
⋮						
∞	(α) 0.4194 ...	(α) 0.4194 ...	$\left(\frac{\alpha}{3}\right)$ 0.1398 ...	$\left(\frac{\alpha}{21}\right)$ 0.0199 ...	$\left(\frac{\alpha}{315}\right)$ 0.0013 ...	$\left(\frac{\alpha}{9765}\right)$ 0.00004 ...

In diese Tabelle habe ich in Klammern den jeweiligen genauen Wert und daneben den angenäherten Dezimalwert von t_e aufgenommen. Die letzte Zeile dieser Tabelle findet ihre Erklärung im folgenden

Satz III. 1. *Es ist*

$$\lim_{t\to\infty} t_e = \frac{\alpha}{(2^1-1)(2^2-1)\cdots(2^e-1)} \tag{52}$$

(*insbesondere* $\lim t_0 = \lim t_1 = \alpha$), *wobei*

$$\alpha = \prod_{n=1}^{\infty}\left(1 - \frac{1}{2^{2n-1}}\right) = \frac{1}{2}\cdot\frac{7}{8}\cdot\frac{31}{32}\cdots = 0.4194\ldots \tag{53}$$

2. *Es ist* $1_0, 2_0, 3_0, \ldots, t_0, \ldots$ *eine monoton abnehmende Folge, und zwar*

$$1_0 > 2_0 = 3_0 > 4_0 = 5_0 > 6_0 = \cdots.$$

3. *Es ist* $2_1, 4_1, 6_1, \ldots$ *eine monoton abnehmende und* $3_1, 5_1, 7_1, \ldots$ *eine monoton zunehmende Folge, und zwar*

$$2_1 > 4_1 > 6_1 > \cdots; \quad 3_1 < 5_1 < 7_1 < \cdots,$$

während die Glieder der gesamten Folge $2_1, 3_1, 4_1, \ldots$ *abwechselnd ab- und zunehmen:*

$$2_1 > 3_1; \quad 3_1 < 4_1; \quad 4_1 > 5_1; \quad 5_1 < 6_1; \ \ldots$$

4. *Für ein festes* e $(= 2, 3, \ldots)$ *sind* $(e+1)_e$, $(e+3)_e$, $(e+5)_e, \ldots$ *und* $(e+2)_e$, $(e+4)_e$, $(e+6)_e, \ldots$ *monoton zunehmende Folgen, und zwar*

$$(e+1)_e < (e+3)_e < (e+5)_e < \cdots; \quad (e+2)_e < (e+4)_e < (e+6)_e < \cdots,$$

während die Glieder der gesamten Folge $(e+1)_e, (e+2)_e, (e+3)_e, \ldots$ *abwechselnd ab- und zunehmen:*

$$(e+1)_e > (e+2)_e; \quad (e+2)_e < (e+3)_e; \quad (e+4)_e < (e+5)_e; \ldots$$

5. *Für ein festes* t $(= 2, 3, \ldots)$ *ist* $t_0, t_1, t_2, \ldots$ *eine monoton abnehmende Folge, und zwar*

$$t_e \leqq \frac{t_{e-1}}{2^e - 1} \qquad (e = 1, 2, 3, \ldots), \tag{54}$$

wobei das Gleichheitszeichen dann und nur dann gilt, wenn $t - e$ *ungerade ist. Insbesondere ist also* $t_0 = t_1$ *für* $2 \mid t$ *und* $t_0 > t_1$ *für* $2 \nmid t$.

6. *Für* $e \geqq 1$ *ist*

$$t_e = \frac{q}{2^{\binom{e+1}{2}}} \left(1 - \frac{1}{2^{e+1}} \leqq q < \frac{3}{2}\right). \tag{55}$$

7. *Es ist* $2_0 + 2_1, 3_0 + 3_1, 4_0 + 4_1, \ldots$ *eine monoton abnehmende Folge, und zwar*

$$(1 = 1_0 =)\ 2_0 + 2_1 > 3_0 + 3_1 = 4_0 + 4_1 > 5_0 + 5_1 = \cdots (> 2\alpha = 0.8388\ldots).$$

In diesem Satze habe ich die auffälligsten Eigenschaften der Wahrscheinlichkeitszahlen t_e zusammengestellt. 7. kann als eine Ergänzung zu 2. und 3. betrachtet werden. Hinsichtlich der Bedeutung der gefundenen Eigenschaften von t_e verweise ich auf die Einleitung. Hier bemerke ich nur noch, daß wegen 5. für jedes t diejenigen Fälle am häufigsten sind, wo es in der absoluten Klassengruppe keine durch 4 teilbare Invariante gibt. Nur für $2 \mid t$ sind auch die Fälle mit genau einer durch 4 teilbaren Invarianten gleich häufig.

Beweis. Wenn t gegen unendlich strebt, nähern sich Zähler und Nenner des zweiten Faktors in (51) den Werten

$$\frac{\prod_{n=1}^{\infty}\left(1 - \frac{1}{2^n}\right)}{\prod_{n=1}^{e}\left(1 - \frac{1}{2^n}\right)} \quad \text{bzw.} \quad \prod_{n=1}^{\infty}\left(1 - \frac{1}{2^{2n}}\right).$$

Der hier auftretende Nenner liefert mit $2^{\binom{e+1}{2}}$ multipliziert den Nenner in (52), während der Quotient der beiden unendlichen Produkte gleich α in (53) ist. Daraus folgt die Richtigkeit von 1. (Der Fall $e = 0$ beansprucht dabei insofern eine besondere Behandlung, als dann das hier auftretende endliche Produkt durch 1 zu ersetzen ist.)

Ich führe die Abkürzung $\left(1 - \frac{1}{2^z}\right)_*$ ein, worunter ich den eingeklammerten Ausdruck verstehe, wenn z eine positive gerade Zahl ist, sonst soll dieses Zeichen den Wert 1 haben. Auf Grund von (51) (und (51a)) erhält man leicht die folgenden Formeln:

$$(t+1)_e = \frac{1 - \frac{1}{2^t}}{\left(1 - \frac{1}{2^{t-e}}\right)_*} t_e, \tag{56}$$

$$(t+2)_e = \frac{\left(1 - \frac{1}{2^{t+1}}\right)\left(1 - \frac{1}{2^t}\right)}{\left(1 - \frac{1}{2^{2\left[\frac{t-e+1}{2}\right]}}\right)} t_e, \tag{57}$$

$$t_{e+1} = \frac{1}{2^{e+1}-1}\left(1 - \frac{1}{2^{t-e-1}}\right)_* t_e, \tag{58}$$

$$(t+1)_{e+1} = \frac{1}{2^{e+1}-1}\left(1 - \frac{1}{2^t}\right) t_e, \tag{59}$$

welche im allgemeinen für $0 \leqq e < t-1$ gültig sind, nur in (58) muß man $0 \leqq e \leqq t-2$ voraussetzen.

Aus (56) folgt sofort $(t+1)_e < t_e$ für $2 \nmid t-e$, $(t+1)_0 = t_0$ für $2 \mid t$ und $(t+1)_e > t_e$ für $2 \mid t-e$, $e > 0$. Zum Beweis von 2., 3., 4. brauchen wir nur noch zu zeigen, daß $(t+2)_1 < t_1$ für $2 \mid t$, $(t+2)_1 > t_1$ für $2 \nmid t$ und $(t+2)_e > t_e$ für $e \geqq 2$ ist. Dies folgt leicht aus (57), da $(t+2)_e = \left(1 - \frac{1}{2^{t+1}}\right) t_e$ für $e = 1$, $2 \mid t$ ist, während für $e = 1$, $2 \nmid i$ und für $e \geqq 2$

$$(t+2)_e > \frac{\left(1 - \frac{1}{2^{t+1}}\right)\left(1 - \frac{1}{2^t}\right)}{1 - \frac{1}{2^{t-1}}} t_e = \frac{2^{2t+1} - 3 \cdot 2^t + 1}{2^{2t+1} - 4 \cdot 2^t} t_e > t_e.$$

Auch 5. folgt leicht aus (58).

Aus 3. folgt die Ungleichung $3_1 < t_1 < 2_1$ $(t \geqq 4)$. Nach (51) ist $3_1 = \frac{3}{8}$, $2_1 = \frac{1}{2}$, woraus (55) für den Fall $e = 1$ folgt. Im Falle $e \geqq 2$ ergibt sich aus 4. und 1. die Ungleichung

$$(e+2)_e < t_e < (\lim t_e =) \frac{\alpha}{(2^1-1)(2^2-1)\cdots(2^e-1)} \qquad (t \geqq e+3).$$

Daraus folgt wegen (51a) für $t \geqq e+3$, daß das q in (55) der Ungleichung

$$1 - \frac{1}{2^{e+1}} < q < \frac{\alpha}{\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{2^2}\right)\cdots\left(1 - \frac{1}{2^e}\right)}$$

genügt. Diese Ungleichung bleibt bestehen, wenn man rechts e ins Unendliche wachsen läßt. Nach (53) steht dann rechts der reziproke Wert des Produkts

$$\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{4^2}\right)\left(1 - \frac{1}{4^3}\right)\cdots$$

Dies ist größer als $\frac{2}{3}$, woraus $q < \frac{3}{2}$ folgt. Für die restlichen Fälle $t = e+1$, $e+2$ erhalten wir für q in (55) direkt aus (51a) die Werte 1 bzw. $1 - \frac{1}{2^{e+1}}$, womit 6. bewiesen ist.

Für $2 \mid t$ folgt aus 2. und 3. die Ungleichung $t_0 + t_1 > (t+1)_0 + (t+1)_1$. Zum Beweis von 7. braucht man also nur noch zu zeigen, daß für $2 \nmid t$ an Stelle dieser Ungleichung eine Gleichung tritt. Dies ist tatsächlich der Fall, da jetzt aus (58), (56), (59) $t_1 = \left(1 - \frac{1}{2^{t-1}}\right) t_0$, $(t+1)_0 = (t+1)_1 = \left(1 - \frac{1}{2^t}\right) t_0$ folgt. Damit ist der Satz bewiesen.

10. Ich definiere für $t = 1, 2, 3, \ldots$

$$M_t(e_4) = \lim_{t \to \infty} \frac{\Sigma e_4}{D(x,t)}, \tag{60}$$

wobei über alle $D \leqq x$ mit dem festen t zu summieren ist und $D(x,t)$ wieder die Anzahl

dieser D bedeutet. Dann ist $M_t(e_4)$ ein Mittelwert im Sinne der Einleitung. Für ihn gilt folgender Satz:

Satz IV. *Für jedes $t = 1, 2, 3, \ldots$ existiert der Mittelwert $M_t(e_4)$ der Anzahl der durch 4 teilbaren Invarianten in der absoluten Klassengruppe derjenigen reell-quadratischen Körper, deren Diskriminante aus t verschiedenen positiven Primfaktoren $\not\equiv 3 \pmod 4$ zusammengesetzt ist, und es ist*

$$M_t(e_4) = \sum_{e=1}^{t-1} e t_e, \tag{61}$$

wobei t_e durch (51), (51a) *gegeben ist. Es ist*

$$(0 =)\ M_1(e_4) < M_2(e_4) < M_3(e_4) < \cdots < M_t(e_4) < \cdots \tag{62}$$

und

$$\lim_{t\to\infty} M_t(e_4) = \alpha \sum_{e=1}^{\infty} \frac{e}{(2^1-1)(2^2-1)\cdots(2^e-1)} = 0.764\ldots, \tag{63}$$

wobei α durch (53) *gegeben ist.*

Merkwürdig ist, daß trotz des in Satz III unter 3., 4. beschriebenen wechselnden Verhaltens von t_e die Folge $M_t(e_4)$ $(t = 1, 2, 3, \ldots)$ nach (62) monoton zunimmt.

Beweis. Der Zähler in (60) läßt sich offenbar in der Form $\sum_{e=0}^{t-1} eD(x, t, e)$ schreiben, wobei $D(x, t, e)$ die bei (29) eingeführte Anzahl ist. Da der Grenzwert in (29) nach dem Satze II existiert, folgt sofort die Richtigkeit von (61). Daraus und aus (52) folgt (63), da die hier auftretende unendliche Reihe konvergent ist.

Bis zum Index $t = 4$ ist (62) richtig, denn es ist nach leichter Rechnung (s. die Tabelle auf S. 34) $M_1(e_4) = 0$, $M_2(e_4) = \frac{1}{2}$, $M_3(e_4) = \frac{5}{8}$, $M_4(e_4) = \frac{45}{64}$. Es ist noch zu beweisen, daß

$$M_t(e_4) < M_{t+1}(e_4) \qquad (t \geqq 4).$$

Ich beweise sogar:

$$\sum_{e=1}^{t-1} t_e \leqq \sum_{e=1}^{t} (t+1)_e \qquad (t \geqq 2) \tag{64}$$

und

$$\sum_{e=2}^{t-1} (e-1) t_e < \sum_{e=2}^{t} (e-1)(t+1)_e \qquad (t \geqq 4), \tag{65}$$

und aus diesen Ungleichungen folgt dann die Behauptung wegen (61) durch Addition.

Nach der Definition ist nämlich $t_0 + t_1 + \cdots + t_{t-1} = 1$, woraus folgt, daß die linke Seite in (64) gleich $1 - t_0$ ist. Die rechte Seite ist ebenso $1 - (t+1)_0$. Da nach 2. von Satz III $t_0 \geqq (t+1)_0$, ist (64) richtig.

Statt (65) beweise ich mit Rücksicht auf das Spätere etwas allgemeiner folgendes:

Wenn $a_2, a_3, a_4, \ldots$ positive Zahlen sind und

$$1 - \frac{1}{e} \leqq \frac{a_e}{a_{e+1}} < 1 \qquad (e = 2, 3, 4, \ldots), \tag{66}$$

so ist

$$a_e t_e + a_{e+1} t_{e+1} < a_e (t+1)_e + a_{e+1} (t+1)_{e+1} \qquad (2 \mid e;\ 2 \leqq e \leqq t-1;\ t \geqq 4), \tag{67}$$

wobei diese Ungleichung im Falle $e = t - 1$ so zu verstehen ist, daß das zweite Glied der linken Seite (d. h. das sinnlose t_t) durch 0 zu ersetzen ist. (Selbstverständlich haben die Zahlen a_e mit den t_e nichts zu tun.)

Da für $a_e = e - 1$ (66) offenbar richtig ist, wird aus der Richtigkeit der Behauptung in (67) durch Addition für $e = 2, 4, 6, \ldots$ (bis $t - 1$ bzw. $t - 2$, je nachdem $2 \nmid t$ oder $2 \mid t$) die Ungleichung (65) folgen.

Das zu beweisende (67) können wir wegen $a_e > 0$ in der Form

$$t_{e+1} - (t+1)_{e+1} < \frac{a_e}{a_{e+1}}((t+1)_e - t_e)$$

schreiben. Indem wir hier (56), (58), (59) einsetzen und durch t_e dividieren, erhalten wir nach leichter Rechnung, den Fällen $2 \mid t$ und $2 \nmid t$ entsprechend (wobei immer $2 \mid e$ zu beachten ist), die Ungleichungen

$$\frac{1}{2^{e+1}-1} \cdot \frac{1}{2^t} < \frac{a_e}{a_{e+1}} \cdot \frac{2^e - 1}{2^t - 2^e}$$

bzw.

$$\frac{1}{2^{e+1}-1}\left(\frac{1}{2^t} - \frac{1}{2^{t-e-1}}\right) < \frac{a_e}{a_{e+1}}\left(-\frac{1}{2^t}\right).$$

Hiervon entsteht die zweite auch im Falle $e = t-1$ (d. h. $t_{e+1} = 0$) durch eine richtige Umformung, da dann $\frac{1}{2^{t-e-1}} = 1$ ist.

Die erste dieser Ungleichungen ist sogar dann richtig, wenn darin $\frac{a_e}{a_{e+1}}$ durch den nach (66) kleineren Wert $1 - \frac{1}{e}$ und der Nenner $2^t - 2^e$ durch 2^t ersetzt wird, denn es ist $\frac{1}{2^{e+1}-1} < \left(1 - \frac{1}{e}\right)(2^e - 1)$ für $e \geqq 2$. Die linke Seite der zweiten Ungleichung ist einfach $-\frac{1}{2^t}$. Auch diese Ungleichung ist wegen (66) richtig, womit die Behauptung in (67) und der Satz IV bewiesen ist.

III. Teil.

11. Ich verstehe unter $\left(\frac{a}{b}\right)_4$ das bekannte rationale vierte Potenzrestsymbol. Dabei sind also a, b ganz und rational, für jeden positiven Primfaktor p von b gilt $p \not\equiv 3 \pmod 4$ und $\left(\frac{a}{p}\right) = 1$; $\left(\frac{a}{p}\right)_4$ ist dann $+1$ bzw. -1, je nachdem für $p \neq 2$ die Kongruenz $z^4 \equiv a \pmod p$ und für $p = 2$ die Kongruenz $z^4 \equiv a \pmod{2^4}$ in ganzem rationalen z lösbar oder unlösbar ist; $\left(\frac{a}{b}\right)_4$ soll für den Nenner die gewöhnliche multiplikative Eigenschaft haben.

Wenn Δ eine D-Zerfällung zweiter Art und zwar $\Delta = D', D''$ ist, so führe ich die Zahlen

$$\alpha'_\Delta = \left(\frac{D'}{D''}\right)_4, \qquad \alpha''_\Delta = \left(\frac{D''}{D'}\right)_4 \tag{68}$$

ein. Unser Ziel ist zunächst, über die zu einem D gehörigen Zahlen $\alpha'_\Delta, \alpha''_\Delta$ einige Hilfssätze zu gewinnen. Dazu brauchen wir eine einfache Vorbereitung, die sich auf die Gruppe aller D-Zerfällungen bezieht.

Es ist bequem, die folgenden Bezeichnungen zu gebrauchen:

Wenn $\Delta_k, \Delta_l, \Delta_m, \ldots$ irgendwelche D-Zerfällungen sind, so soll $\Delta_{klm}\ldots$ die daraus zusammengesetzte D-Zerfällung $\Delta_k \Delta_l \Delta_m \cdots$ bezeichnen.

C soll die Untermengen von $(1, 2, \ldots, e)$, darunter auch die leere Menge bedeuten, wobei e eine feste positive ganze Zahl ist. Ähnlich sollen $C_a, C^a, C_{ab}, C^b_a, \ldots$ diejenigen C bedeuten, die a enthalten, a nicht enthalten, a und b enthalten, a enthalten und b nicht enthalten, ..., wobei $a, b, \ldots$ verschiedene Elemente von $(1, 2, \ldots, e)$ sind.

Dann gilt der folgende

Hilfssatz E. *Wenn* $\Delta_1, \Delta_2, \ldots, \Delta_e$ $(1 \leqq e \leqq t)$ *beliebig gegebene D-Zerfällungen sind und zwar* $\Delta_s = D_s', D_s''$ $(s = 1, 2, \ldots, e)$, *so lassen sich die positiven ganzen Zahlen* d_C $(C < (1, 2, \ldots, e))$ *eindeutig so bestimmen, daß die Gleichungen*

$$D_s' = \prod_{C_s} d_{C_s}, \quad D_s'' = \prod_{C^s} d_{C^s} \qquad (s = 1, 2, \ldots, e) \tag{69}$$

erfüllt sind. Wie auch eine Untergruppe G' *der Ordnung* 2^e *in der Gruppe aller D-Zerfällungen gegeben ist, stets läßt sich in ihr eine Basis* $\Delta_1, \Delta_2, \ldots, \Delta_e$ *so wählen, daß in* (69) $d_1, d_2, \ldots, d_e > 1$ *sind. Wenn dabei* G' *das Element* $\Delta^* = D, 1$ *nicht enthält, so gibt es eine Gruppe* G'' *von derselben Ordnung* 2^e, *die* Δ^* *auch nicht enthält, für die außerdem* $\{G'', \Delta^*\} = \{G', \Delta^*\}$ *ist, so daß nach Ersetzung von* G' *durch* G'' *sogar* $d_0, d_1, d_2, \ldots, d_e > 1$ *erreichbar ist.* (In d_0 bedeutet 0 die leere Menge.)

Wegen der Forderungen (69) muß nämlich d_C für ein beliebiges C den folgenden Bedingungen genügen: $d_C \mid D_s'$ $(s \in C)$, $d_C \mid D_s''$ $(s \notin C)$ für $s = 1, 2, \ldots, e$. Und zwar sieht man, daß d_C der größte gemeinsame Teiler der jetzt genannten D_s' und D_s'' sein muß. Wenn nämlich ein p_k aus den Primfaktoren von $D = p_1 p_2 \cdots p_t$ (dies ist wieder die Bezeichnung wie in **4**) in *denselben* D_s' und D_s'' aufgeht und dabei $p_k \nmid d_C$ wäre, so muß ein anderes $d_{C'}$ mit $C' \neq C$ durch p_k teilbar sein, da das Produkt aller d_C wegen (69) offenbar gleich D ist. Entweder gibt es nun ein z, das in C' enthalten und in C nicht enthalten ist, woraus wegen $p_k \mid d_{C'}$ nach dem obigen $p_k \mid D_z'$, d. h. $p_k \nmid D_z''$ folgt, was der Voraussetzung über p_k widerspricht, oder es gibt ein z, das in C, aber nicht in C' enthalten ist, woraus ähnlich der Widerspruch $p_k \mid D_z'$, d. h. $p_k \nmid D_z''$ folgt.

Umgekehrt sieht man leicht, daß (69) erfüllt ist, wenn d_C als größter gemeinsamer Teiler der obigen D_s' $(s \in C)$, D_s'' $(s \notin C)$ definiert ist. Damit ist bewiesen, daß die Darstellung in (69) möglich und eindeutig ist.

Nun sei $\Delta_1, \Delta_2, \ldots, \Delta_e$ eine unabhängige Basis einer Gruppe G' von D-Zerfällungen. Es sei p_k ein Teiler von D_1', der wegen $D_1' > 1$ gewiß existiert. Indem ich Δ_s $(s = 2, 3, \ldots, e)$ je nach Bedarf durch $\Delta_1 \Delta_s = \Delta_s'$ ersetze und die neue (unabhängige) Basis wieder mit $\Delta_1, \ldots, \Delta_e$ bezeichne, kann ich erreichen, daß $p_k \nmid D_s'$ ist $(s = 2, 3, \ldots, e)$. Dann ist wegen (69) $p_k \mid d_1$; denn jedenfalls ist $p_k \mid d_C$ mit einem gewissen C, das 1 enthalten muß (da sonst $p_k \nmid D_1'$ wäre), das aber kein $s \neq 1$ enthalten kann (da sonst $p_k \mid D_s'$ wäre). Ich wähle dann einen Teiler p_l von D_2'. Nun multipliziere ich je nach Bedarf die Elemente $\Delta_1, \Delta_3, \Delta_4, \ldots, \Delta_e$ mit Δ_2. Wenn ich die neue Basis, die so entsteht, wieder mit $\Delta_1, \ldots, \Delta_e$ bezeichne, verliert p_k seine frühere Eigenschaft nicht. Dabei läßt sich erreichen, daß p_l außer in D_2' in keinem anderen D_s' aufgeht. D. h. $p_k \mid d_1$ bleibt erhalten, und hierzu kommt analog noch $p_l \mid d_2$. Offenbar erhält man auf solchem Wege $d_1, d_2, \ldots, d_e > 1$.

Zum folgenden bemerke ich zunächst, daß die D-Zerfällung $\Delta^* = D, 1$ bei der Zusammensetzung mit einer beliebigen D-Zerfällung $\Delta = D', D''$ die Vertauschung der Glieder D', D'' bewirkt, d. h. $\Delta\Delta^* = D'', D'$.

Wenn nun G' das Element Δ^* nicht enthält, dann ist zunächst $\Delta^*, \Delta_1, \Delta_2, \ldots, \Delta_e$ eine unabhängige Basis der Gruppe $G^* = \{G', \Delta^*\}$. Ich ersetze Δ_s $(s = 1, 2, \ldots, e)$ je nach Bedarf durch $\Delta_s \Delta^*$ und bezeichne die so erhaltene neue Basis von G^* wieder mit $\Delta^*, \Delta_1, \ldots, \Delta_e$, so daß für das neue System $\Delta_1, \ldots, \Delta_e$, das wieder die unabhängige Basis einer Gruppe G'' bildet, z. B. $p_1 \mid D_s''$ $(s = 1, 2, \ldots, e)$ gilt. Daraus folgt nach (69) $p_1 \mid d_0$, d. h. $d_0 > 1$. Offenbar gilt dies auch dann, wenn wir $\Delta_1, \Delta_2, \ldots, \Delta_e$ einer ähnlichen Umformung unterwerfen wie oben, so daß dann $d_0, d_1, \ldots, d_e > 1$ sind. Da ferner $\{G'', \Delta^*\} = \{G', \Delta^*\}$ gilt, ist der Hilfssatz E bewiesen.

Wir beweisen jetzt den

Hilfssatz F. *Gegeben sei eine Untergruppe G' von der Ordnung 2^e ($e \geqq 1$) der Gruppe aller D-Zerfällungen, die aus lauter D-Zerfällungen zweiter Art besteht und das Element $\Delta^* = D, 1$ nicht enthält. Dann gilt:*

1. *Ist $\Delta_1, \Delta_2, \ldots, \Delta_e$ eine (unabhängige) Basis von G' und durchläuft Δ alle Elemente von G' in einer festen Reihenfolge, so ist das aus α'_Δ, α''_Δ entstandene System durch das System $\mathsf{A} = (\alpha'_{\Delta_1}, \alpha'_{\Delta_2}, \ldots, \alpha'_{\Delta_e};\ \alpha''_{\Delta_1}, \alpha''_{\Delta_2}, \ldots, \alpha''_{\Delta_e};\ \alpha'_{\Delta_{12}}, \alpha'_{\Delta_{13}}, \ldots, \alpha'_{\Delta_{e-1,e}})$ bestimmt, wobei im Falle $e = 1$ unter A einfach $(\alpha'_{\Delta_1}, \alpha''_{\Delta_1})$ zu verstehen ist.* (In diesem Falle ist die Behauptung trivial.)

2. *Dann und nur dann ist für alle Elemente Δ von G'*

$$\alpha'_\Delta \cdot \alpha''_\Delta = 1, \tag{70}$$

wenn das Gleiche für die unabhängigen Basiselemente $\Delta_1, \Delta_2, \ldots, \Delta_e$ von G' gilt.

3. *Für alle von der D-Zerfällung $1, D$ verschiedenen Elemente Δ von G' kann*

$$\alpha'_\Delta = \alpha''_\Delta = -1 \tag{71}$$

nur dann bestehen, wenn $e = 1$ oder 2 ist.

Wir beweisen zunächst die folgenden Identitäten:

$$\alpha'_{\Delta_1}\alpha''_{\Delta_1}\alpha'_{\Delta_2}\alpha''_{\Delta_2}\alpha'_{\Delta_{12}}\alpha''_{\Delta_{12}} = 1, \tag{72}$$

$$\alpha^{(k)}_{\Delta_1}\alpha^{(k)}_{\Delta_2}\alpha^{(k)}_{\Delta_3}\alpha^{(k)}_{\Delta_{12}}\alpha^{(k)}_{\Delta_{13}}\alpha^{(k)}_{\Delta_{23}}\alpha^{(k)}_{\Delta_{123}} = 1 \qquad (k = 1, 2), \tag{73}$$

wobei $\Delta_1, \Delta_2, \Delta_3$ beliebige D-Zerfällungen zweiter Art sind.

Nach (69) kann man nämlich $\Delta_1 = d_1 d_{12}, d_0 d_2$; $\Delta_2 = d_2 d_{12}, d_0 d_1$ setzen, wobei d_0, d_1, d_2, d_{12} positive ganze Zahlen sind. Dann ist $\Delta_{12} = \Delta_1\Delta_2 = d_1 d_2, d_0 d_{12}$. Die linke Seite von (72) lautet also

$$\left(\frac{d_1 d_{12}}{d_0 d_2}\right)_4 \left(\frac{d_0 d_2}{d_1 d_{12}}\right)_4 \left(\frac{d_2 d_{12}}{d_0 d_1}\right)_4 \left(\frac{d_0 d_1}{d_2 d_{12}}\right)_4 \left(\frac{d_1 d_2}{d_0 d_{12}}\right)_4 \left(\frac{d_0 d_{12}}{d_1 d_2}\right)_4.$$

Durch Anwendung der Regeln $\left(\frac{x}{yz}\right)_4 = \left(\frac{x}{y}\right)_4 \left(\frac{x}{z}\right)_4$, $\left(\frac{x}{z}\right)_4 \left(\frac{y}{z}\right)_4 = \left(\frac{xy}{z}\right)_4$ erhalten wir daraus

$$\left(\frac{(d_1 d_2 d_{12})^2}{d_0}\right)_4 \left(\frac{(d_0 d_2 d_{12})^2}{d_1}\right)_4 \left(\frac{(d_0 d_1 d_{12})^2}{d_2}\right)_4 \left(\frac{(d_0 d_1 d_2)^2}{d_{12}}\right).$$

Wegen $\left(\frac{x^2}{y}\right)_4 = \left(\frac{x}{y}\right)$ können wir gleichzeitig die Exponenten 2 und die Indizes 4 streichen, wodurch ein Ausdruck entsteht, der sich mit Hilfe des quadratischen Reziprozitätsgesetzes in 1 überführen läßt. Damit ist (72) bewiesen.

Zum Beweis von (73) setzen wir ebenfalls nach (69) $\Delta_1 = d_1 d_{12} d_{13} d_{123}, d_0 d_2 d_3 d_{23}$; $\Delta_2 = d_2 d_{12} d_{23} d_{123}, \ldots$; $\Delta_3 = d_3 d_{13} d_{23} d_{123}, \ldots$, wobei an Stelle der Punkte jedesmal das Produkt aus den übrigen vier $d_0, d_1, \ldots$ einzusetzen ist. Wir führen der Einfachheit halber die Bezeichnung $d_0 = m$, $d_1 = a$, $d_2 = b$, $d_3 = c$, $d_{12} = x$, $d_{13} = y$, $d_{23} = z$, $d_{123} = n$ ein. Dann ist $\Delta_1 = ayzn, \ldots$; $\Delta_2 = bxzn, \ldots$; $\Delta_3 = cxyn, \ldots$ mit ähnlicher Abkürzung. Daraus folgt

$\Delta_{12} = \Delta_1\Delta_2 = abxy, \ldots$; $\Delta_{13} = acxz, \ldots$; $\Delta_{23} = bcyz, \ldots$; $\Delta_{123} = \Delta_{12}\Delta_3 = abcn, \ldots$

Für $k = 1$ läßt sich also die linke Seite von (73) so schreiben:

$$\left(\frac{ayzn}{mbcx}\right)_4 \left(\frac{bxzn}{macy}\right)_4 \left(\frac{cxyn}{mabz}\right)_4 \left(\frac{abxy}{mczn}\right)_4 \left(\frac{acxz}{mbyn}\right)_4 \left(\frac{bcyz}{maxn}\right)_4 \left(\frac{abcn}{mxyz}\right)_4.$$

Dieser Ausdruck läßt sich auf ähnlichem Wege wie oben in

$$\prod_{u,v} \left(\frac{u^2}{v}\right)_4 \cdot \left(\frac{(abcxyzn)^4}{m}\right)_4$$

überführen, wobei u, v alle Paare mit zwei verschiedenen Elementen aus $m, a, \ldots, z, n$ zu durchlaufen hat. Offenbar haben hier beide Faktoren für sich den Wert 1, womit (73) im Falle $k = 1$ bewiesen ist. Der Fall $k = 2$ läßt sich ähnlich behandeln. (Dieser Fall ist übrigens leicht auf den Fall $k = 1$ zurückzuführen, wenn wir noch (72) zu Hilfe nehmen.)

Nun soll $\Delta_1, \Delta_2, \ldots, \Delta_e$ eine unabhängige Basis für G' bezeichnen, wobei G' die Voraussetzungen des Hilfssatzes erfüllt. Wir wollen zunächst 1. beweisen. Dann dürfen wir also $e \geqq 2$ annehmen. Wir wenden (72) auf Δ_l, Δ_m (statt Δ_1, Δ_2) an, wobei l, m zwei beliebige verschiedene Zahlen aus $1, 2, \ldots, e$ sind. Nach der erhaltenen Gleichung läßt sich $\alpha''_{\Delta_{lm}}$ aus $\alpha'_{\Delta_l}, \alpha'_{\Delta_m}, \alpha''_{\Delta_l}, \alpha''_{\Delta_m}, \alpha'_{\Delta_{lm}}$, also aus dem System

$$\mathsf{A} = (\alpha'_{\Delta_1}, \ldots;\ \alpha''_{\Delta_1}, \ldots;\ \ldots, \alpha'_{\Delta_{e-1,e}})$$

ausrechnen. Ähnliches folgt für $\alpha'_{\Delta_{lmn}}, \alpha''_{\Delta_{lmn}}$ aus (73), wenn dies auf $\Delta_l, \Delta_m, \Delta_n$ angewandt wird $(1 \leqq l < m < n \leqq e)$. Dann wenden wir (73) auf $\Delta_l, \Delta_m, \Delta_{ns}$ an $(1 \leqq l < m < n < s \leqq e)$, und so fortfahrend erhalten wir das Gleiche für alle $\alpha^{(k)}_{\Delta_{lmn}\ldots}$. Da jedes Element von G' außer $\Delta = 1, D$ unter $\Delta_{lmn}\ldots$ vorkommt und für $\Delta = 1, D$ offenbar $\alpha'_\Delta = \alpha''_\Delta = 1$ ist, haben wir 1. bewiesen.

Wenn wir die vorige Bezeichnung $\Delta_1, \Delta_2, \ldots, \Delta_e$ weiter beibehalten und für diese Elemente die Richtigkeit von (70) voraussetzen, so folgt die Richtigkeit wegen (72) auch für $\Delta_{lm}\,(1 \leqq l < m \leqq e)$. Multipliziert man die Gleichungen (73) für $k = 1, 2$, so kann man daraus wie bei dem Beweis von 1. nacheinander auf die Gültigkeit von (70) für $\Delta_{lmn}, \Delta_{lmns}, \ldots$ schließen. Da für $\Delta = 1, D$ immer $\alpha'_\Delta \alpha''_\Delta = 1$ ist, folgt die Behauptung 2.

Endlich folgt die Behauptung 3. aus (73). Wenn nämlich $e \geqq 3$ ist, so gibt es drei unabhängige Elemente $\Delta_1, \Delta_2, \Delta_3$ in G'. Diese und die daraus zusammengesetzten D-Zerfällungen $\Delta_{12}, \Delta_{13}, \Delta_{23}, \Delta_{123}$ sind alle von $1, D$ verschieden. Für alle diese D-Zerfällungen kann (71) wegen (73) nicht bestehen, weil nämlich auf der linken Seite die Anzahl der Faktoren ungerade ist. Damit ist der Hilfssatz F bewiesen.

Der Teil 1. dieses Hilfssatzes wird seine Ergänzung im folgenden Hilfssatze finden, aus dem wir später folgern werden, daß das System A in gewissem Sinne unabhängig ist.

Hilfssatz G. *Es seien e und t positive ganze Zahlen, $1 \leqq e \leqq t - 1$. Es seien $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t; \mathfrak{p}'_1, \ldots, \mathfrak{p}'_t$ insgesamt $2t$ Symbole, für die ich vorläufig nur formal $n(\mathfrak{p}_k) = p_k$ $(k = 1, 2, \ldots, t)$ setze. Weiter bedeute δ_C (C Teilmenge von $(1, 2, \ldots, e)$) ein (formales) Produkt aus einigen verschiedenen $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ (eventuell $\delta_C = 1$) derart, daß das Produkt aller δ_C gleich $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_t$ und $\delta_0, \delta_1, \ldots, \delta_e \neq 1$ ist. Es sei noch $d_C = n(\delta_C)$. Ich setze endlich*

$$(74)\quad P = \prod_{1 \leqq u < v \leqq t} \left(\frac{p_u}{\mathfrak{p}_v}\right)_i^{m_{uv}} \prod_{k=1}^{e} \left(\frac{\Pi d_{C_k}}{\Pi \delta_{C^k}}\right)_{i4}^{a_k} \prod_{k=1}^{e} \left(\frac{\Pi d_{C^k}}{\Pi \delta_{C_k}}\right)_{i4}^{b_k} \prod_{1 \leqq k < l \leqq e} \left(\frac{\Pi d_{C_k^l} \Pi d_{C_l^k}}{\Pi \delta_{C_{kl}} \Pi \delta_{C^{kl}}}\right)_i^{c_{kl}},$$

wobei unter den inneren Produktzeichen $C_k, C^k, C_{kl}, \ldots$ alle C zu durchlaufen hat, die k enthalten, k nicht enthalten, k und l enthalten, ... und $m_{uv}\,(1 \leqq u < v \leqq t)$, a_k, b_k $(1 \leqq k \leqq e)$, $c_{kl}\,(1 \leqq k < l \leqq e)$ alle 0 oder 1 sind, jedoch soll wenigstens eine 1 unter ihnen vorkommen. (Wenn $e = 1$ ist, ist das vierte Produkt wegzulassen.)

Dann gibt es eine ganze rationale Zahl r $(2 \leqq r \leqq t)$, ein Potenzprodukt $\mathfrak{a}$ aus $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_{r-1}; \mathfrak{p}'_1, \ldots, \mathfrak{p}'_{r-1}$, das keine (formale) vierte Potenz ist, und ein Produkt $\overline{P}$ aus beliebigen Symbolen $\left(\frac{y}{z}\right)_{i4}$, in die für y, z je zwei verschiedene der $\mathfrak{p}_1, \ldots, \mathfrak{p}_{r-1}; \mathfrak{p}'_1, \ldots, \mathfrak{p}'_{r-1}$

einzusetzen sind (eventuell $\bar{P} = 1$*) derart, daß*

$$P = \bar{P}\left(\frac{\mathfrak{p}_r}{\mathfrak{a}}\right)_{i4} \tag{75}$$

ist, wie auch immer $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ *durch primäre Primzahlen ersten Grades in* $R(i)$ *so ersetzt werden, daß dabei* $p_1, p_2, \ldots, p_t$ *verschieden sind.* (Natürlich bedeuten bei dieser Einsetzung der Strich bzw. das n die Zeichen für die Konjugierten- bzw. Normenbildung und $(-)_i$, $(-)_{i4}$ das zweite und vierte Potenzrestsymbol in $R(i)$.

Zum Beweis nehme ich wie vereinbart an, daß in (74) statt $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ schon Primzahlen in $R(i)$ eingesetzt wurden. Ich werde dann die rechte Seite von (74) gewissen Umformungen unterwerfen, die ich *zulässige* Umformungen nenne, nämlich:

$$\left(\frac{\alpha\beta}{\gamma}\right)_{i4} = \left(\frac{\alpha}{\gamma}\right)_{i4}\left(\frac{\beta}{\gamma}\right)_{i4}, \quad \left(\frac{\alpha}{\beta\gamma}\right)_{i4} = \left(\frac{\alpha}{\beta}\right)_{i4}\left(\frac{\alpha}{\gamma}\right)_{i4}, \quad \left(\frac{\alpha}{\beta}\right)_{i4} = \left(\frac{\alpha'}{\beta'}\right)_{i4}^{3}, \quad \left(\frac{\alpha}{\beta}\right)_{i4}^{4} = 1, \quad \left(\frac{\alpha}{\beta}\right)_{i} = \left(\frac{\alpha}{\beta}\right)_{i4}^{2},$$

wo α, β, γ ganze Zahlen in $R(i)$ sind, für die die vorkommenden Symbole einen Sinn haben, und $\left(\frac{\alpha}{\beta}\right)_{i4} = \left(\frac{\beta}{\alpha}\right)_{i4}$ ist, wenn außerdem α und β primär sind und eins von ihnen rational oder eine Quadratzahl in $R(i)$ ist. Alle diese Gleichungen dürfen als zulässige Umformungen in beiden Richtungen angewandt werden. Davon ist die letzte ein Sonderfall des biquadratischen Reziprozitätsgesetzes (s. z. B. a. a. O. [6]), S. 106, III). Die zulässigen Umformungen verändern den Wert der rechten Seite von (74) offenbar nicht, gleichgültig wie $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ gewählt wurden.

Nun können wir die rechte Seite von (74) durch zulässige Umformungen auf die Form eines Produkts aus einigen $\left(\frac{p_k}{\mathfrak{p}_l}\right)_{i4}$ bringen. Dann können wir diese Faktoren zulässig so umformen, daß darin $p_s, \mathfrak{p}_s'$ überhaupt nicht und $\mathfrak{p}_s$ auch nie im Nenner vorkommt, wobei s eine beliebige feste Zahl von $1, 2, \ldots, t$ ist. Hierbei haben wir es nämlich nur mit solchen Faktoren $\left(\frac{p_k}{\mathfrak{p}_l}\right)_{i4}$ zu tun, in denen $k = s$ oder $l = s$ ist. Wegen

$$\left(\frac{p_s}{\mathfrak{p}_l}\right)_{i4} = \left(\frac{\mathfrak{p}_s}{\mathfrak{p}_l}\right)_{i4}\left(\frac{\mathfrak{p}_s'}{\mathfrak{p}_l}\right)_{i4} = \left(\frac{\mathfrak{p}_s}{\mathfrak{p}_l}\right)_{i4}\left(\frac{\mathfrak{p}_s}{\mathfrak{p}_l'}\right)_{i4}^{3} \tag{76}$$

und

$$\left(\frac{p_k}{\mathfrak{p}_s}\right)_{i4} = \left(\frac{\mathfrak{p}_s}{p_k}\right)_{i4} \tag{76a}$$

ist dann die Behauptung klar. Sodann vereinigen wir das Produkt aller solchen Faktoren $\left(\frac{\mathfrak{p}_s}{\mathfrak{p}_k}\right)_{i4}, \left(\frac{\mathfrak{p}_s}{\mathfrak{p}_k'}\right)_{i4}, \left(\frac{\mathfrak{p}_s}{p_k}\right)_{i4}$ $(k \neq s; 1 \leqq k \leqq t)$ zu $\left(\frac{\mathfrak{p}_s}{\mathfrak{a}_s}\right)_{i4}$, wobei $\mathfrak{a}_s$ ein Potenzprodukt aus den $\mathfrak{p}_k, \mathfrak{p}_k'$ $(k \neq s; 1 \leqq k \leqq t)$ ist, in dem alle Exponenten mod 4 reduziert (d. h. durch eine der Zahlen 0, 1, 2, 3 ersetzt) werden können. Damit hat man P in (74) als Produkt aus $\left(\frac{\mathfrak{p}_s}{\mathfrak{a}_s}\right)_{i4}$ und einigen $\left(\frac{p_k}{\mathfrak{p}_l}\right)_{i4}$ $(k, l \neq s)$ dargestellt. Eine olche Darstellung von P, wo also $\mathfrak{a}_s$ keine vierte Idealpotenz enthält, nenne ich *in bezug auf* $\mathfrak{p}_s$ *reduziert*, $\mathfrak{a}_s$ selbst einen *reduzierten Nenner zu* $\mathfrak{p}_s$. Im obigen wurde also gezeigt, daß es in bezug auf jedes $\mathfrak{p}_s$ eine reduzierte Darstellung von P gibt. Offenbar gehört zu jedem $\mathfrak{p}_s$ ein einziger reduzierter Nenner. Wenn nämlich auch $\mathfrak{m}$ ein solcher ist, so läßt sich $\left(\frac{\mathfrak{p}_s}{\mathfrak{a}_s \mathfrak{m}^{-1}}\right)_{i4}$ (in multiplikativem

Sinne!) aus den zwei reduzierten Darstellungen als ein Produkt von einigen $\left(\frac{p_k}{\mathfrak{p}_l}\right)_{i4}$ $(k, l \neq s)$ ausdrücken, was nur möglich ist, wenn $\mathfrak{a}_s \mathfrak{m}^{-1}$ eine vierte Idealpotenz, d. h. $\mathfrak{m} = \mathfrak{a}_s$ ist.

Ich behaupte, daß es unter den reduzierten Nennern $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_t$ wenigstens einen $\neq 1$ gibt.

Ich zeige zunächst, daß aus dieser Behauptung der Hilfssatz G folgt. Wir reduzieren nämlich P in (74) in bezug auf $\mathfrak{p}_t$. Ist $\mathfrak{a}_t \neq 1$, so ist der Hilfssatz richtig (und zwar $r = t$). Ist aber $\mathfrak{a}_t = 1$, so fällt der Faktor $\left(\frac{\mathfrak{p}_t}{\mathfrak{a}_t}\right)_{i4}$ völlig aus, und wir haben daher P als ein Produkt einiger $\left(\frac{p_k}{\mathfrak{p}_l}\right)_{i4}$ $(k \neq l;\ 1 \leqq k, l \leqq t-1)$ dargestellt. Mit Hilfe von (76), (76a) können wir daraus eine reduzierte Darstellung von P in bezug auf $\mathfrak{p}_{t-1}$ erhalten. Ist der erhaltene reduzierte Nenner $\mathfrak{a}_{t-1} \neq 1$, so ist der Hilfssatz richtig $(r = t-1)$. Sonst ist P ein Produkt einiger $\left(\frac{p_k}{\mathfrak{p}_l}\right)_{i4}$ $(k \neq l;\ 1 \leqq k, l \leqq t-2)$. Damit können wir analog verfahren. Wenn wir nicht eher zum Ziele kommen, finden wir auf diesem Wege mit Hilfe zulässiger Umformungen die Darstellung $P = \left(\frac{\mathfrak{p}_2}{\mathfrak{a}_2}\right)_{i4}$, wobei also $\mathfrak{a}_2$ der reduzierte Nenner zu $\mathfrak{p}_2$ ist, der nur aus Faktoren $\mathfrak{p}_1, \mathfrak{p}_1'$ besteht. Dieses $\mathfrak{a}_2$ muß aber $\neq 1$ sein, woraus der Hilfssatz G (mit $r = 2$) folgt. Wäre nämlich $\mathfrak{a}_2 = 1$, so wäre (nach zulässigen Umformungen) $P = 1$, d. h. $\mathfrak{a}_1 = \mathfrak{a}_2 = \cdots = \mathfrak{a}_t = 1$, entgegen der Behauptung.

Wir brauchen also nur noch die obige Behauptung zu beweisen. Dazu nehmen wir an, daß die reduzierten Nenner $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_t$ alle gleich 1 sind, um daraus einen Widerspruch abzuleiten.

Nach der Annahme ist $\delta_0, \delta_1, \ldots, \delta_e \neq 1$. Wir dürfen annehmen, daß $\mathfrak{p}_t \mid \delta_0, \mathfrak{p}_s \mid \delta_s$ $(s = 1, 2, \ldots, e)$, da es jetzt auf diese Bezeichnungsweise offenbar nicht ankommt. Wir wählen ein bestimmtes $s (= 1, 2, \ldots, t)$ und suchen den reduzierten Nenner zu $\mathfrak{p}_s$ unmittelbar nach (74) darzustellen. Dies kann folgendermaßen geschehen: Wir lassen in (74) jeden Faktor $(-)_i$ und $(-)_{i4}$ fort, wo weder der Zähler durch p_s noch der Nenner durch $\mathfrak{p}_s$ teilbar ist. Dann ersetzen wir die übriggebliebenen Faktoren der Gestalt $\left(\frac{a}{\beta}\right)_{i4}$ (a rational, β in $R(i)$) durch $\left(\frac{p_s}{\beta}\right)_{i4}$ für $p_s \mid a$ und durch $\left(\frac{a}{\mathfrak{p}_s}\right)_{i4}$ für $\mathfrak{p}_s \mid \beta$. (All dies bedeutet nur, daß wir die Bestandteile fortlassen, die auf $\mathfrak{a}_s$ nicht einwirken.) Sodann multiplizieren wir die übriggebliebenen Faktoren der Gestalt $\left(\frac{p_s}{\mathfrak{p}_k}\right)_i$, $\left(\frac{p_k}{\mathfrak{p}_s}\right)_i$, $\left(\frac{p_s}{\beta}\right)_{i4}$, $\left(\frac{a}{\mathfrak{p}_s}\right)_{i4}$, jede Art für sich, miteinander, wodurch aus der rechten Seite von (74) ein Ausdruck

$$\left(\frac{p_s}{\xi_s}\right)_i \left(\frac{x_s}{\mathfrak{p}_s}\right)_i \left(\frac{p_s}{\eta_s}\right)_{i4} \left(\frac{y_s}{\mathfrak{p}_s}\right)_{i4}$$

entsteht. Wir können auf den dritten und vierten Faktor eine ähnliche Gleichung anwenden wie (76) und (76a), und auch die ersten zwei Faktoren lassen sich ähnlich umformen, wenn wir vorher $(-)_{i4}^2$ statt $(-)_i$ schreiben. Wir gewinnen also:

$$\mathfrak{a}_s = \xi_s^2 \xi_s'^2 x_s^2 \eta_s \eta_s'^3 y_s; \tag{77}$$

diese Gleichung ist nur bis auf vierte Idealpotenzfaktoren richtig, was aber für unsere Zwecke genügt. (Hier bedeuten ξ_s', η_s' selbstverständlich die Konjugierten von ξ_s und η_s.)

Von diesen Größen $\xi_s, \ldots, y_s$ rechnen wir nur y_s für $s = 1, 2, \ldots, e$ und für $s = t$, ferner η_t aus.

Beim Ausrechnen von y_s $(s = 1, 2, \ldots, e)$ aus (74) müssen wir berücksichtigen, daß $\mathfrak{p}_s \mid \delta_s$ ist, und zwar in δ_s nur zur ersten Potenz aufgeht, während natürlich $\mathfrak{p}_s \nmid \delta_C$ für $C \neq s$. Wir erhalten also aus (74):

$$y_s = \prod_{\substack{k=1 \\ k \neq s}}^{e} (\Pi d_{C_k})^{a_k} \quad (\Pi d_{C^s})^{b_s} \prod_{\substack{1 \leq k < l \leq e \\ k, l \neq s}} (\Pi d_{C_k^l} \Pi d_{C_l^k})^{c_{kl}} \qquad (s = 1, 2, \ldots, e), \tag{78}$$

wobei in den inneren Produkten wieder über alle $C_k, C^s, \ldots$ zu multiplizieren ist.

Für $s = t$ gewinnen wir ähnlich wegen $\mathfrak{p}_t \mid \delta_0, \mathfrak{p}_t \nmid \delta_C$ $(C \neq 0)$:

$$y_t = \prod_{k=1}^{e} (\Pi d_{C_k})^{a_k} \prod_{1 \leq k < l \leq e} (\Pi d_{C_k^l} \Pi d_{C_l^k})^{c_{kl}} \tag{79}$$

und

$$\eta_t = \prod_{k=1}^{e} (\Pi \delta_{C_k})^{b_k}. \tag{80}$$

Nun ist wegen (77), da x_s, y_s rational sind, $\mathfrak{a}_s \mathfrak{a}_s'^{-1} = (\eta_s' \eta_s^{-1})^2$. Da wir $\mathfrak{a}_s$ in (77) nur bis auf vierte Idealpotenzfaktoren genau ausgedrückt haben, lautet die ursprüngliche Voraussetzung für das (veränderte) $\mathfrak{a}_s$ in (77) so: $\mathfrak{a}_s$ $(s = 1, 2, \ldots, t)$ ist vierte Idealpotenz. Da η_s, η_s' teilerfremd sind (denn η_s ist ein Produkt aus gewissen primären Primzahlen $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ in $R(i)$, worunter es keine konjugierten gibt), so folgt aus der vorigen Gleichung, daß $\eta_s' \eta_s^{-1}$, d. h. auch η_s ein Idealquadrat ist. Aus (77) folgt dann noch, daß auch y_s ein Idealquadrat, d. h. eine rationale Quadratzahl ist.

Da η_t ein Idealquadrat ist, enthält η_t insbesondere $\mathfrak{p}_k$ $(k = 1, 2, \ldots, e)$ zur geraden Potenz. Der Exponent von $\mathfrak{p}_k$ in η_t läßt sich auf Grund von (80) leicht bestimmen. Dazu müssen wir nochmals $\mathfrak{p}_k \mid \delta_k, \mathfrak{p}_k \nmid \delta_C$ $(C \neq k)$ berücksichtigen (dabei ist $\mathfrak{p}_k^2 \nmid \delta_k$). Dieser Exponent ist b_k. Dies soll also gerade sein. Da $b_k = 0, 1$ angenommen war, folgt

$$b_k = 0 \qquad (k = 1, 2, \ldots, e). \tag{81}$$

Da y_t eine rationale Quadratzahl ist und offenbar $p_j \mid d_j, p_j^2 \nmid d_j, p_j \nmid d_C$ $(C \neq j)$ für $j = 1, 2, \ldots, e$, können wir leicht aus (79) durch Zusammenzählen des genauen Exponenten von p_j in y_t auf die folgende Kongruenz schließen:

$$a_j + \sum_{\substack{1 \leq k < l \leq e \\ k \text{ oder } l = j}} c_{kl} \equiv 0 \pmod 2 \qquad (j = 1, 2, \ldots, e). \tag{82}$$

Endlich ist auch y_s $(s = 1, 2, \ldots, e)$ eine rationale Quadratzahl. Verfahren wir mit den Primzahlen p_j $(j \neq s;\ 1 \leqq j \leqq e)$ ähnlich wie früher, indem wir noch (81) berücksichtigen, so erhalten wir die Kongruenz:

$$a_j + \sum_{\substack{1 \leq k < l \leq e \\ k, l \neq s \\ k \text{ oder } l = j}} c_{kl} \equiv 0 \pmod 2 \qquad (j, s = 1, 2, \ldots, e;\ j \neq s). \tag{83}$$

Durch Subtraktion folgt aus (82) und (83) c_{js} oder $c_{sj} \equiv 0 \pmod 2$, je nachdem $j < s$ oder $j > s$ ist. Wegen $c_{kl} = 0, 1$ folgt also $c_{kl} = 0$ $(1 \leqq k < l \leqq e)$. Dann folgt aus (82) $a_j \equiv 0 \pmod 2$, d. h. wegen $a_j = 0, 1$ folgt $a_j = 0$ $(j = 1, 2, \ldots, e)$.

Wegen (81) und des eben Bewiesenen geht also (74) in

$$P = \prod_{1 \leq u < v \leq t} \left(\frac{p_u}{\mathfrak{p}_v} \right)_i^{m_{uv}}$$

über, wobei wenigstens ein Exponent m_{uv} gleich 1 ist. Ist r der größte Wert von v mit $m_{uv} = 1$, wobei also $2 \leqq r \leqq t$ ist, so läßt sich P wegen(76a) in der Form

$$P = \prod_{1 \leqq u < v \leqq r-1} \left(\frac{p_u}{\mathfrak{p}_v}\right)_i^{m_{uv}} \cdot \left(\frac{\mathfrak{p}_r}{\mathfrak{a}}\right)_{i4}$$

schreiben mit $\mathfrak{a} = (p_1^{m_{1r}} p_2^{m_{2r}} \cdots p_{r-1}^{m_{r-1,r}})^2$. Es ist also $\mathfrak{a}$ der reduzierte Nenner zu $\mathfrak{p}_r$ und offenbar keine vierte Idealpotenz in $R(i)$, entgegen der Voraussetzung. Damit ist der Hilfssatz G bewiesen.

12. Ich nehme D wieder in der Form $p_1 p_2 \cdots p_t$ (wie in **4**) an und betrachte alle D von einem festen quadratischen Typus T. G_2 sei die Gruppe aller D-Zerfällungen zweiter Art, die jetzt wieder für alle solche D aufzufassen sind, wie es am Ende von **5** auseinandergesetzt war. Ich lasse Δ alle Elemente von G_2 in einer festen Reihenfolge durchlaufen und betrachte das System U, das aus T und aus allen Zahlen α'_Δ, α''_Δ in (68) besteht. Ich nenne U den biquadratischen Typus von D.

Zu jedem biquadratischen Typus U gehört also ein bestimmter quadratischer Typus T, der ein Teilsystem von U ist. Anders gesagt, jedes D vom biquadratischen Typus U ist zugleich von diesem quadratischen Typus T.

Nach (28) enthält U außer den Elementen von T 2^{e_4+2} Elemente α'_Δ, α''_Δ, die alle gleich ± 1 sind. Darunter gibt es aber viele Elemente, die voneinander abhängig sind. Zunächst sind α'_Δ, α''_Δ immer gleich 1, wenn $\Delta = 1, D$ oder $D, 1$. Weiter ist $\alpha'_\Delta = \alpha''_{\Delta_1}$ (und $\alpha''_\Delta = \alpha'_{\Delta_1}$), wenn Δ und Δ_1 sich nur durch die Reihenfolge der Glieder unterscheiden ($\Delta = D', D''$; $\Delta_1 = D'', D'$). Bestimmen wir also eine Untergruppe G' von G_2, die das Element $\Delta^* = D, 1$ nicht enthält und für die $G_2 = \{G', \Delta^*\}$ ist, so haben wir für U jedenfalls alle Möglichkeiten erschöpft, wenn wir nur die zu den Elementen $\Delta(\neq 1, D)$ von G' gehörigen α'_Δ, α''_Δ betrachten: Denn Δ und $\Delta\Delta^*$ unterscheiden sich, wie schon bemerkt, nur durch die Reihenfolge der Glieder. Da G' die Ordnung 2^{e_4} hat, ist die Anzahl dieser α'_Δ, α''_Δ immer noch $2(2^{e_4} - 1)$. Nun sind diese Elemente nach 1. von Hilfssatz F alle durch die $2e_4 + \binom{e_4}{2}$ Elemente des Systems $\mathsf{A} = (\alpha'_{\Delta_1}, \ldots, \alpha'_{\Delta_e}; \alpha''_{\Delta_1}, \ldots, \alpha''_{\Delta_e}; \alpha'_{\Delta_{12}}, \ldots, \alpha'_{\Delta_{e-1,e}})$ bestimmt, wo $e = e_4$ zu setzen ist und $\Delta_1, \Delta_2, \ldots, \Delta_e$ eine unabhängige Basis von G' bedeutet. Daß keine Einschränkung mehr möglich ist, wird im folgenden Satze ausgedrückt, der also eine Umkehrung von 1. des Hilfssatzes F ist.

Satz V. *Es sei ein quadratischer Typus T vorgegeben, für den $e_4 = e$ $(= 0, 1, \ldots, t-1)$ ist, ferner eine (beliebige) Untergruppe G' der Gruppe G_2 aller D-Zerfällungen zweiter Art, die die D-Zerfällung $\Delta^* = D, 1$ nicht enthält und für die $\{G', \Delta^*\} = G_2$ ist, die also die Ordnung 2^e hat, und eine (beliebige) unabhängige Basis $\Delta_1, \Delta_2, \ldots, \Delta_e$ für G'.*

Der biquadratische Typus U von D vom quadratischen Typus T ist durch das System $\mathsf{A} = (\alpha'_{\Delta_1}, \ldots, \alpha'_{\Delta_e}; \alpha''_{\Delta_1}, \ldots, \alpha''_{\Delta_e}; \alpha'_{\Delta_{12}}, \alpha'_{\Delta_{13}}, \ldots, \alpha'_{\Delta_{e-1,e}})$ bestimmt. Wie auch Werte ± 1 für die Elemente von A vorgeschrieben sind, immer gibt es solche D, für die A dieses Wertsystem annimmt. Die Anzahl der (zu diesem T gehörigen) U ist also $2^{2e+\binom{e}{2}} = 2^{\frac{e(e+3)}{2}}$.

Ist (wie früher) $D(x, T)$ die Anzahl der $D \leqq x$ vom quadratischen Typus T und sind darunter $D(x, U)$ vom biquadratischen Typus U, so ist unabhängig von U

$$\lim_{x \to \infty} \frac{D(x, U)}{D(x, T)} = \frac{1}{2^{\frac{e(e+3)}{2}}}. \tag{84}$$

Kurz gesagt bestimmt also dieser Satz die Anzahl der wirklich vorhandenen U zu einem beliebigen T und behauptet überdies, daß alle diese U (innerhalb T) gleich

wahrscheinlich sind. Im Falle $e_4 = 0$ ist der Satz wohl richtig, aber inhaltslos, da dann offenbar nur ein einziges U existiert. Im Falle $e_4 = 1$ ist unter A das System $(\alpha'_{\Delta_1}, \alpha''_{\Delta_1})$ zu verstehen.

Beim Beweise dürfen wir $(e_4 =)\ e \geqq 1$ annehmen, woraus $t \geqq 2$ folgt. Ich beweise zuerst die letzte Behauptung des Satzes. Wir wählen vorläufig die Gruppe G' und die Basis $\Delta_1, \Delta_2, \ldots, \Delta_e$, wie es im Satze angenommen war, insbesondere so, daß dafür in (69) $d_0, d_1, \ldots, d_e > 1$ ist, was nach dem Hilfssatz E möglich ist. Der vorgegebene quadratische Typus T sei durch $\left(\frac{p_u}{p_v}\right) = x_{uv} (1 \leqq u < v \leqq t)$ gegeben, wo also $x_{uv} (= \pm 1)$ irgendwelche feste Zahlen sind. Dann wähle ich nach Belieben feste Zahlen y'_k, y''_k $(k = 1, 2, \ldots, e)$ und $z_{kl} (1 \leqq k < l \leqq e)$, die alle gleich 1 oder -1 sind. Ich setze danach

$$(85)\quad g = \prod_{1 \leqq u < v \leqq t} \frac{1}{2}\left(1 + x_{uv}\left(\frac{p_u}{p_v}\right)\right) \prod_{k=1}^{e} \frac{1}{2}\left(1 + y'_k \alpha'_{\Delta_k}\right) \prod_{k=1}^{e} \frac{1}{2}\left(1 + y''_k \alpha''_{\Delta_k}\right) \prod_{1 \leqq k < l \leqq e} \frac{1}{2}\left(1 + z_{kl} \alpha'_{\Delta_{kl}}\right).$$

Wenn ich hier ein $D = p_1 p_2 \cdots p_t$ vom quadratischen Typus T einsetze, hat der erste Faktor den Wert 1, und offenbar hat g den Wert 1 oder 0, je nachdem das Gleichungssystem $\alpha'_{\Delta_k} = y'_k$, $\alpha''_{\Delta_k} = y''_k (k = 1, 2, \ldots, e)$, $\alpha'_{\Delta_{kl}} = z_{kl} (1 \leqq k < l \leqq e)$ erfüllt ist oder nicht. Nun ist durch diese Gleichungen ein biquadratischer Typus U definiert, zu dem der quadratische Typus T gehört, wie es oben besprochen war (und auch unmittelbar aus 1. im Hilfssatz F folgt). Es ist also

$$(86)\qquad D(x, U) = \sum_{D \leqq x} g,$$

wobei die Summe über alle $D \leqq x$ vom quadratischen Typus T zu erstrecken ist. Die Existenz eines zu einem beliebigen System y'_k, y''_k, z_{kl} gehörigen U ist noch nicht bewiesen. Gerade dies ist eine Teilbehauptung des Satzes. Anders gesagt, es ist noch möglich, daß die Summe in (86) verschwindet, was gerade bedeuten würde, daß das betreffende U nicht existiert. Wenn wir aber zeigen, daß $D(x, U)$, für das wir (86) als Definitionsgleichung betrachten, nie Null ist und auch (84) gilt, dann haben wir die letzte Behauptung des Satzes bewiesen.

Wegen Satz I lautet die Behauptung (84) offenbar

$$(87)\qquad \lim_{x \to \infty} \frac{D(x, U)}{D(x, t)} = \frac{1}{2^{\binom{t}{2} + \frac{e(e+3)}{2}}}.$$

Wir brauchen also nur zu beweisen, daß (87) für (86) gilt. In (86) dürfen wir die geraden D außer acht lassen, da deren Anzahl, wie schon erwähnt war, ein $O\left(\frac{x (\log \log x)^{t-2}}{\log x}\right)$ ist, und für den Nenner auf der linken Seite von (87) die Relation (23) besteht. Ich forme dann den Summanden g in (86) folgendermaßen um. Ich wähle nach Belieben t primäre Primzahlen $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ ersten Grades in $R(i)$ so, daß $n(\mathfrak{p}_k) = p_k$ $(k = 1, 2, \ldots, t)$ ist. In allen Symbolen $(-)$, $(-)_4$, die in (85) vorkommen und bei denen natürlich (68) eingesetzt zu denken ist, ersetze ich im Nenner jedes p_k durch $\mathfrak{p}_k$, so daß dann diese Symbole in $R(i)$ zu betrachten, d. h. alle mit dem Index i zu versehen sind. Bekanntlich verändert dabei kein solches Symbol seinen Wert, insbesondere die vorkommenden α'_Δ, α''_Δ deswegen nicht, weil hier alle D-Zerfällungen Δ von der zweiten Art sind, für die also in (68) der Zähler ein quadratischer Rest vom Nenner ist. Dadurch geht g in eine Funktion von $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ über, wobei dieses System genau so definiert ist, wie am

Anfang von **I** (insbesondere ist $n(\mathfrak{p}_1) < n(\mathfrak{p}_2) < \cdots < n(\mathfrak{p}_t)$). Entsprechend ist dann in (86) über alle solche Systeme $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$, d. h. im Sinne von **I** über alle solche $\mathfrak{P}_t = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_t$ zu summieren, welche jetzt neben $n(\mathfrak{P}_t) \leqq x$ noch dadurch eingeschränkt sind, daß alle Normen $n(\mathfrak{P}_t)$ verschieden sein sollen (oder, was auf dasselbe hinauskommt, von den konjugierten Primzahlen $\mathfrak{p}_k$ nur die zugelassen sind, die z. B. einen positiven Imaginärteil haben), und $D = n(\mathfrak{P}_t)$ vom quadratischen Typus T sein soll. Das Aufheben der ersten Einschränkung ist gleichbedeutend mit dem Hinzutreten des Faktors 2^t, da g nach dem Vorigen davon unabhängig ist, wie die $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ aus den konjugierten Größen gewählt worden sind. Die zweite Einschränkung läßt sich ohne weiteres aufheben. Wenn nämlich $n(\mathfrak{P}_t) = D$ nicht vom quadratischen Typus T ist, d. h. für wenigstens ein Paar u, v $(1 \leqq u < v \leqq t)$ $\left(\frac{p_u}{\mathfrak{p}_v}\right)_i = \left(\frac{p_u}{p_v}\right) + x_{uv}$ ist, dann ist g nach (85) des ersten Faktors wegen gleich 0. Führen wir also statt (86) die Funktion

$$f(x) = \sum_{n(\mathfrak{P}_t) \leqq x} g \tag{88}$$

ein, wobei g schon in Symbole $(-)_i$ und $(-)_{i4}$ umgeschrieben zu denken ist, so genügt es, statt (87) die Gleichung

$$\lim_{x \to \infty} \frac{f(x)}{D(x,t)} = \frac{2^t}{2^{\binom{t}{2} + \frac{e(e+3)}{2}}} \tag{89}$$

zu beweisen.

Nach (85) ist

$$g = \frac{1}{2^{\binom{t}{2} + \frac{e(e+3)}{2}}} \left(1 + \sum_P (\pm P)\right),$$

wobei P alle nichtleeren Produkte aus verschiedenen $\left(\frac{p_u}{p_v}\right)$, α'_{Δ_k}, α''_{Δ_k}, $\alpha'_{\Delta_{kl}}$ in (85) zu durchlaufen hat (hierfür sind nachher noch Symbole $(-)_i$, $(-)_{i4}$ einzuführen).

Nun ist

$$\sum_{n(\mathfrak{P}_t) \leqq x} 1 \sim 2^t D(x,t),$$

wie wir beim Beweise von Satz I gesehen haben. Wenn wir also noch

$$\sum_{n(\mathfrak{P}_t) \leqq x} P = O\left(\frac{x(\log\log x)^{t-2}}{\log x}\right) \tag{90}$$

nachweisen, so haben wir wegen (23), (88) die Behauptung (89) bewiesen.

Dazu haben wir die Struktur von P zu prüfen. Ich schreibe Δ_k wieder in der Form D', D'' und stelle D', D'' für $k = 1, 2, \ldots, e$ durch die d_C in (69) dar, wo dann nach der Voraussetzung $d_0, d_1, \ldots, d_e > 1$ ist. Wenn ich noch $\Delta_{kl} (= \Delta_k \Delta_l) = D'_{kl}, D''_{kl}$ setze, so folgt aus (69) offenbar

$$D'_{kl} = \Pi d_{C_k^l} \Pi d_{C_l^k}, \quad D''_{kl} = \Pi d_{C_{kl}} \Pi d_{C^{kl}} \qquad (1 \leqq k < l \leqq e). \tag{91}$$

Die Faktoren von P werden nach (68) durch

$$\left(\frac{p_u}{p_v}\right), \left(\frac{D'_k}{D''_k}\right)_4, \left(\frac{D''_k}{D'_k}\right)_4, \left(\frac{D'_{kl}}{D''_{kl}}\right)_4$$

dargestellt, wobei (69) und (91) einzusetzen und nachher zu Symbolen $(-)_i$ und $(-)_{i4}$ überzugehen ist. Damit erhält P offenbar die Form in (74), und zwar mit Exponenten m_{uv}, a_k, b_k, c_{kl}, die alle gleich 0 oder 1 sind, unter denen aber wenigstens eine 1 vorkommt, wie es dort angenommen war. Nach dem Hilfssatz G läßt sich also P in der Form (75)

schreiben. Somit ist P so definiert, wie c in (3), woraus nach (4) und (5) die Behauptung (90) folgt. Damit ist der letzte Teil des Satzes V bewiesen.

Aus dem eben bewiesenen Teil folgt insbesondere, daß die genaue Anzahl der wirklich existierenden biquadratischen Typen U (zu einem T) gleich $2^{\frac{e(e+3)}{2}}$ ist. Ich betrachte jetzt eine beliebige feste Untergruppe G' von G_2, wie im Satze vorgegeben, und eine beliebige unabhängige Basis $\Delta_1, \Delta_2, \ldots, \Delta_e$ von ihr. Da das System

$$\mathsf{A} = (\alpha'_{\Delta_1}, \ldots; \alpha''_{\Delta_1}, \ldots; \ldots, \alpha'_{\Delta_{e-1,e}})$$

aus $\frac{e(e+3)}{2}$ Elementen besteht, ist auch die Anzahl der wirklich existierenden A höchstens $2^{\frac{e(e+3)}{2}}$; wir müssen nämlich damit rechnen, daß die Elemente von A nicht unabhängig sind. Nun bestimmt jedes U als Teilsystem von ihm ein A, und zu zwei verschiedenen U gehören nach 1. von Hilfssatz F verschiedene A. Die Anzahl der letzteren muß also auch $2^{\frac{e(e+3)}{2}}$ sein und zwischen den A und U besteht eine ein-eindeutige Zuordnung. Damit ist der Satz V völlig bewiesen.

13. Aus der Arbeit R (S. 147—148) zitiere ich zwei Sätze, die ich nachher auch als Satz$^-$ und Satz$^+$ bezeichnen werde. Unter Umständen bestimmen diese Sätze aus dem biquadratischen Typus U von D das Vorzeichen der Norm der Grundeinheit des Körpers $R(\sqrt{D})$. Ich bezeichne diese Grundeinheit mit ε (es kommt hier nicht darauf an, welche von den vier Grundeinheiten gewählt wird), und auch im Körper $R(\sqrt{D})$ soll n die Norm bezeichnen. Diese Sätze lauten dann folgendermaßen (im ersten Satze ist die letzte Bemerkung eine unmittelbare Folgerung aus 3. von Hilfssatz F und (28), die bisher außer acht gelassen war):

Satz VI (oder **Satz$^-$**). *Ist für alle D-Zerfällungen* $\Delta(\mp 1, D; D, 1)$ *von der zweiten Art*

$$\alpha'_\Delta = \alpha''_\Delta = -1, \tag{92}$$

so ist $n(\varepsilon) = -1$. *Insbesondere ist also im Falle* $e_4 = 0$ (*wo es kein* Δ *gibt*) *immer* $n(\varepsilon) = -1$. *Im Falle* $e_4 \geqq 3$ *ist dieser Satz nicht anwendbar, da dann* (92) *nicht für jedes* Δ *bestehen kann.*

Satz VII (oder **Satz$^+$**). *Gibt es eine D-Zerfällung* Δ *der zweiten Art, für die*

$$\alpha'_\Delta \alpha''_\Delta = -1 \tag{93}$$

ist, so ist $n(\varepsilon) = +1$ [10]).

Ich werde jetzt prüfen, wie oft diese Sätze anwendbar sind. Ich wähle einen festen quadratischen Typus T, womit also auch ein t gegeben ist. Dann bezeichne ich mit $D(X, T, -)$ die Anzahl der $D \leqq x$ vom quadratischen Typus T, für die der Satz$^-$ sich anwenden läßt. Entsprechend sei auch $D(x, T, +)$ definiert. Ich setze

$$T^- = \lim_{x\to\infty} \frac{D(x, T, -)}{D(x, T)} \tag{94}$$

und

$$T^+ = \lim_{x\to\infty} \frac{D(x, T, +)}{D(x, T)}. \tag{95}$$

Entsprechend soll $D(x, t, -)$ und $D(x, t, +)$ die Anzahl von $D \leqq x$ mit festem t bedeuten, für die der Satz$^-$ bzw. Satz$^+$ anwendbar ist. Ich setze dann

---

[10]) In beiden Sätzen ist $\alpha'_\Delta, \alpha''_\Delta$ gemäß (68) zu verstehen. Es ist ferner zu berücksichtigen, daß ich in der Arbeit R die D-Zerfällungen D', D'' und D'', D' als nicht verschieden angesehen habe.

$$t^- = \lim_{x\to\infty} \frac{D(x,t,-)}{D(x,t)} \tag{96}$$

und

$$t^+ = \lim_{x\to\infty} \frac{D(x,t,+)}{D(x,t)}. \tag{97}$$

Diese Grenzwerte T^-, T^+, t^-, t^+ bedeuten also die Wahrscheinlichkeit der Fälle, in denen der Satz$^-$ bzw. der Satz$^+$ anwendbar ist, unter allen Körpern $R(\sqrt{D})$, deren Diskriminante D vom quadratischen Typus T ist bzw. genau t verschiedene Primzahlfaktoren hat.

Endlich bezeichne ich mit $T^?$ und $t^?$ die entsprechende Wahrscheinlichkeit der Fälle, in denen keiner dieser Sätze anwendbar ist (d. h. das Vorzeichen von $n(\varepsilon)$ fraglich bleibt), die also durch

$$T^? = 1 - T^- - T^+ \tag{98}$$

und

$$t^? = 1 - t^- - t^+ \tag{99}$$

definiert werden können.

Natürlich ist unser Hauptziel, t^-, t^+ und damit $t^?$ zu bestimmen. Dies geschieht am einfachsten so, daß wir zunächst T^- und T^+ bestimmen. Es wird übrigens nicht ohne Interesse sein, die Wahrscheinlichkeit für die Anwendbarkeit von Satz$^-$ und Satz$^+$ auch in den Fällen zu kennen, die durch je ein T (aus allen D mit festem t) ausgesondert sind. Auch die Wahrscheinlichkeiten $T^?, t^?$ beanspruchen für sich ein volles Interesse, da sie einen Überschlag darüber geben, wie oft diese Sätze die Norm von ε unaufgeklärt lassen; diese Zahlen drücken sozusagen aus, in welchem Grade diese Sätze unvollkommen sind. (Dazu ist zu bemerken, daß allem Anscheine nach diese Sätze kaum durch ähnlich einfache Sätze ergänzt werden können [11].)

Es gilt nun der folgende

Satz VIII. *Ist für den quadratischen Typus T die Anzahl e_4 der durch 4 teilbaren Invarianten in der absoluten Klassengruppe der zugehörigen quadratischen Körper gleich e, so ist den Fällen $e = 0, 1, 2$ und $e \geqq 3$ entsprechend $T^- = 1, \frac{1}{4}, \frac{1}{32}$ und 0 und $T^+ = 1 - \frac{1}{2^e}$ für jedes e. Diese Wahrscheinlichkeiten hängen also von T nur insoweit ab, wie $e_4 = e$ von T abhängt.* (Die Aussagen $T^- = 1$, $T^+ = 0$ für $e = 0$ und $T^- = 0$ für $e \geqq 3$ sind in einer stärkeren Formulierung im Satz$^-$ enthalten.)

Ich stelle diese Zahlen T^-, t^+ und auch $T^?$ tabellarisch zusammen:

$e_4 =$	0	1	2	3	4 ...	e ...	$t-1$
$T^- =$	1	$\frac{1}{4}$	$\frac{1}{32}$	0	0 ...	0 ...	0
$T^+ =$	0	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{7}{8}$	$\frac{15}{16}$ ...	$1-\frac{1}{2^e}$ ...	$1-\frac{1}{2^{t-1}}$
$T^? =$	0	$\frac{1}{4}$	$\frac{7}{32}$	$\frac{1}{8}$	$\frac{1}{16}$ ...	$\frac{1}{2^e}$ ...	$\frac{1}{2^{t-1}}$.

(Diese Tabelle ist so zu verstehen, daß man zu jedem T diejenige Kolonne aufsucht, die dem durch T bestimmten Werte von e_4 entspricht.)

[11]) Vgl. A. Scholz, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, Math. Zeitschr. **39** (1934), 93—111.

Beweis. Der Fall $e_4 = 0$ ist bekannt, wir setzen also $e_4 = e \geqq 1$ voraus. Wir bestimmen zunächst T^+. Dazu betrachten wir einen beliebigen festen quadratischen Typus T und wählen ein festes System $\Delta_1, \Delta_2, \ldots, \Delta_e$, wie im Satz V. Ob der Satz$^+$ anwendbar ist, hängt nur vom biquadratischen Typus U ab. Nach Satz V sind alle zu T gehörigen U und alle Systeme A einander eineindeutig zugeordnet. Wegen (84) erhalten wir also T^+, wenn wir die Anzahl aller A bestimmen, für die der Satz$^+$ anwendbar ist, und diese Anzahl durch $2^{\frac{e(e+3)}{2}}$ dividieren.

Diese Anzahl ergibt sich, wenn wir von der Gesamtzahl $2^{\frac{e(e+3)}{2}}$ der A die Anzahl derjenigen A abziehen, für die der Satz$^+$ nicht anwendbar ist, d. h. die Gleichung (93) mit keiner D-Zerfällung Δ der zweiten Art besteht. Die letzteren A sind also diejenigen, für die die Gleichung (70) mit allen solchen Δ gilt. Dazu ist nach 2. von Hilfssatz F notwendig und hinreichend, daß für die insgesamt $\frac{e(e+3)}{2}$ Elemente von

$$\mathsf{A} = (\alpha'_{\Delta_1}, \ldots; \alpha''_{\Delta_1}, \ldots, \alpha'_{\Delta_{e-1,e}})$$

die e Gleichungen $\alpha'_{\Delta_k}\alpha''_{\Delta_k} = 1$ $(k = 1, 2, \ldots, e)$ bestehen. Da sonst die Elemente von A nach Belieben gleich ± 1 sein können, und jetzt über $\frac{e(e+3)}{2} - e = \frac{e(e+1)}{2}$ Elemente frei zu verfügen ist, ist die gesuchte Anzahl gleich $2^{\frac{e(e+3)}{2}} - 2^{\frac{e(e+1)}{2}}$. Dividieren wir dies durch $2^{\frac{e(e+3)}{2}}$, so erhalten wir den behaupteten Wert für T^+.

Für T^- brauchen wir nur die Fälle $e_4 = e = 1, 2$ zu prüfen. Dementsprechend ist die Anzahl der U gleich $2^2 = 4$ bzw. $2^4 = 32$. Auch jetzt können wir ähnlich verfahren wie früher. Es ist also die Anzahl der A zu bestimmen, für die die Gleichungen (92) bestehen, und diese Zahl dann durch 4 bzw. 32 zu dividieren.

Im Falle $e_4 = 2$ gibt es außer 1, D und D, 1, die für (92) nicht in Betracht kommen, nur die D-Zerfällungen $\Delta_1, \Delta_2, \Delta_{12}$ von der zweiten Art, und die daraus durch Vertauschung der Glieder entstehenden D-Zerfällungen. Die Vertauschung der Glieder von Δ bewirkt offenbar nur eine Vertauschung von α'_Δ und α''_Δ in (68), somit fordert (92) nur, daß $\alpha'_{\Delta_1}, \alpha''_{\Delta_1}, \alpha'_{\Delta_2}, \alpha''_{\Delta_2}, \alpha'_{\Delta_{12}}, \alpha''_{\Delta_{12}}$ sämtlich gleich -1 sind. Mit den ersten fünf Zahlen ist nach (72) auch die sechste gleich -1, und diese fünf Zahlen, die nach Satz V frei als ± 1 wählbar sind, bilden genau das System A. Offenbar gibt es also ein einziges A, für das (92) gilt. In diesem Falle $e_4 = 2$ ist also in der Tat $T^- = \frac{1}{32}$.

Der Fall $e_2 = 1$ läßt sich ähnlich behandeln. Jetzt kommt für (92) nur die D-Zerfällung Δ_1 in Betracht, es wird also $\alpha'_{\Delta_1} = \alpha''_{\Delta_1} = -1$ gefordert. Dies bestimmt auch jetzt ein einziges System $\mathsf{A} = (\alpha'_{\Delta_1}, \alpha''_{\Delta_1})$, somit haben wir in diesem Falle $T^- = \frac{1}{4}$. Damit ist Satz VIII bewiesen.

Nunmehr ist es leicht, auch die Wahrscheinlichkeiten $t^-, t^+, t^?$ zu ermitteln. Von diesen läßt sich t^+ so bestimmen: Wir betrachten alle D mit genau t verschiedenen Primfaktoren. Darunter kommt nach Satz I jeder quadratische Typus T mit gleicher Wahrscheinlichkeit vor. Für ein bestimmtes T ist die Wahrscheinlichkeit T^+ für die Anwendbarkeit von Satz$^+$ nur von e_4 abhängig, während e_4 eine Funktion von T allein ist. Und zwar haben die Fälle mit einem festen $e_4 = e$ eine Wahrscheinlichkeit t_e. Somit ist die Wahrscheinlichkeit t^+ für die Anwendbarkeit von Satz$^+$ bei diesem t gleich $\sum_{e=0}^{t-1} t_e T^+$, wo

die Summe so zu verstehen ist, daß in jedem Gliede $t_e T^+$ ein solches T zu nehmen ist, für welches $e_4 = e$ ist. Ähnlich lassen sich t^- und $t^?$ ausdrücken, und so folgt aus Satz VIII der folgende

Satz IX. *Unter allen reell-quadratischen Körpern mit einer aus genau t verschiedenen positiven Primzahlen* ($\equiv 3 \pmod 4$) *bestehenden Diskriminante, haben die Fälle, in denen man mit Hilfe der Sätze* VI *und* VII (*d. h. Satz$^-$ bzw. Satz$^+$*) *auf negative bzw. positive Grundeinheitsnorm schließen kann, und die Fälle unter denselben Körpern, in denen sich das Vorzeichen der Norm der Grundeinheit mit Hilfe dieser Sätze nicht entscheiden läßt, je eine Wahrscheinlichkeit $t^-, t^+, t^?$, die durch die folgenden Formeln gegeben sind:*

$$t^- = t_0 + \frac{1}{4} t_1 + \frac{1}{32} t_2, \tag{100}$$

$$t^+ = \sum_{e=1}^{t-1} \left(1 - \frac{1}{2^e}\right) t_e = 1 - \sum_{e=0}^{t-1} \frac{1}{2^e}\, t_e, \tag{101}$$

$$t^? = \frac{1}{4} t_1 + \frac{7}{32} t_2 + \sum_{e=3}^{t-1} \frac{1}{2^e} t_e, \tag{102}$$

wobei t_e durch (51), (51a) *gegeben ist. In den Fällen $t = 1, 2$ ist statt* (100) *und* (102) $1^- = 1_0 = 1$, $2^- = 2_0 + \frac{1}{4} 2_1 = \frac{5}{8}$, $1^? = 0$, $2^? = \frac{1}{4} 2_1 = \frac{1}{8}$ *zu nehmen.*

Die zweite Form von t^+ in (101) folgt daraus, daß immer $t_0 + t_1 + \cdots + t_{t-1} = 1$ ist.

Eine wichtige Ergänzung dieses Satzes ist der folgende

Satz X. *Es ist* $(1 =)\, 1^- > 2^- > \cdots > t^- > \cdots$ *mit*

$$\lim_{t \to \infty} t^- = \frac{121\alpha}{96} = 0.528\ldots, \tag{103}$$

wobei α die Zahl in (53) *bedeutet.*

Es ist $(0 =)\, 1^+ < 2^+ < \cdots < t^+ < \cdots$ *mit*

$$\lim_{t \to \infty} t^+ = \frac{1}{3} = 0.333\ldots \tag{104}$$

Es ist $(0 =)\, 1^? < 3^? < 5^? < \cdots$ *und* $\left(\frac{1}{8} =\right) 2^? < 4^? < 6^? < \cdots$ *mit*

$$\lim_{t \to \infty} t^? = \frac{64 - 121\alpha}{96} = 0.138\ldots \tag{105}$$

Um einen klaren Überblick über die Größe von $t^-, t^+, t^?$ zu haben, stelle ich hier auf Grund des Satzes IX (mit Hilfe der Tabelle von S. 34) einige Anfangswerte zusammen:

$1^- =$	1	$1^+ =$	0	$1^? =$	0
$2^- = \frac{5}{8}$	$= 0.625$	$2^+ = \frac{1}{4}$	$= 0.25$	$2^? = \frac{1}{8}$	$= 0.125$
$3^- = \frac{153}{256}$	$= 0.597\ldots$	$3^+ = \frac{9}{32}$	$= 0.281\ldots$	$3^? = \frac{31}{256}$	$= 0.121\ldots$
$4^- = \frac{1127}{2048}$	$= 0.550\ldots$	$4^+ = \frac{161}{512}$	$= 0.313\ldots$	$4^? = \frac{277}{2048}$	$= 0.135\ldots$
$5^- = \frac{4459}{8192}$	$= 0.544\ldots$	$5^+ = \frac{5265}{16384}$	$= 0.321\ldots$	$5^? = \frac{2201}{16384}$	$= 0.134\ldots$

Beweis von Satz X. Aus (100), (51), (51a) rechnet man t^- leicht aus:

$$t^- = \frac{121}{96}\left(1 - \frac{\omega}{2^t}\right) \prod_{k=1}^{t-1}{}' \left(1 - \frac{1}{2^k}\right),$$

wobei $\omega = \frac{4}{121}$ bzw. $\frac{50}{121}$ ist, je nachdem $2 \mid t$ oder $2 \nmid t$ ist, und der Strich neben dem Produktzeichen bedeutet, daß die geraden Werte von k auszulassen sind. Für $2 \mid t$ ist also

$$\frac{(t+1)^-}{t^-} = \frac{1 - \frac{25}{121} \cdot \frac{1}{2^t}}{1 - \frac{4}{121} \cdot \frac{1}{2^t}} < 1.$$

Ähnlich ist für $2 \nmid t$

$$\frac{(t+1)^-}{t^-} = \frac{1 - \frac{2}{121} \cdot \frac{1}{2^t}}{1 - \frac{50}{121} \cdot \frac{1}{2^t}} \left(1 - \frac{1}{2^t}\right) < 1.$$

Auch (103) folgt leicht aus (100), wenn man noch bedenkt, daß t_0, t_1, t_2 nach (52) für $t \to \infty$ gegen die Werte $\alpha, \alpha, \frac{\alpha}{3}$ streben.

Die Behauptung $t^+ < (t+1)^+$ ist für $t = 1, 2, 3$ nach der obigen Tabelle richtig. Um sie allgemein zu beweisen, darf ich also im folgenden $t \geqq 4$ voraussetzen. Jedenfalls genügt es auf Grund von (101) zu zeigen, daß

$$(106) \quad \left(1 - \frac{1}{2^e}\right) t_e + \left(1 - \frac{1}{2^{e+1}}\right) t_{e+1} < \left(1 - \frac{1}{2^e}\right) (t+1)_e + \left(1 - \frac{1}{2^{e+1}}\right) (t+1)_{e+1}$$
$$(2 \mid e;\ 2 \leqq e < t;\ t \geqq 4)$$

(wobei im Falle $e = t - 1$ wieder $t_t = 0$ zu setzen ist) und

$$(107) \quad \frac{1}{2} t_1 + \frac{3}{4} t_2 + \frac{7}{8} t_3 < \frac{1}{2} (t+1)_1 + \frac{3}{4} (t+1)_2 + \frac{7}{8} (t+1)_3$$
$$(2 \mid t;\ t \geqq 4),$$

wenn wir noch berücksichtigen, daß nach Satz IV für ungerades t immer $t_1 < (t+1)_1$, d. h. $\frac{1}{2} t_1 < \frac{1}{2} (t+1)_1$ ist. Wenn man nämlich zu dieser Ungleichung die Ungleichungen (106) mit $e = 2, 4, \ldots, t-1$ addiert, dann hat man nach (101) die Ungleichung $t^+ < (t+1)^+$ für ein ungerades t ($\geqq 5$). Ähnliches folgt im Falle eines geraden t ($\geqq 4$) aus (107) und den Ungleichungen (106) mit $e = 4, 6, \ldots, t-2$.

Zum Beweis von (106) setzen wir $a_e = 1 - \frac{1}{2^e}$ (dies a_e soll mit t_e nichts zu tun haben). Dann gilt offenbar $1 - \frac{1}{2^e} < \frac{a_e}{a_{e+1}} < 1$, woraus wegen $1 - \frac{1}{e} < 1 - \frac{1}{2^e}$ ($e \geqq 2$) (66) folgt. Folglich ist auch (67) befriedigt, was jetzt genau (106) ist.

Zum Beweis von (107) wenden wir zunächst auf t_3 und $(t+1)_3$ die Formeln (58) und (59) an, wobei $2 \mid t$ zu berücksichtigen ist. Dann geht (107) nach Multiplikation mit 8 in die folgende Ungleichung über:

$$4t_1 + \left(6 + \frac{1}{2^t}\right) t_2 < 4(t+1)_1 + 6(t+1)_2.$$

Wir wenden jetzt auf t_2, $(t+1)_1$, $(t+1)_2$ die Formeln (58), (56), (59) an, wodurch diese Ungleichung nach Division mit t_1 in

$$4 + \left(6 + \frac{1}{2^t}\right) \cdot \frac{1}{3}\left(1 - \frac{1}{2^{t-2}}\right) < 4\left(1 - \frac{1}{2^t}\right) + 2\left(1 - \frac{1}{2^t}\right)$$

übergeht. Diese Ungleichung läßt sich leicht bestätigen, womit $t^+ < (t+1)^+$ allgemein bewiesen ist.

Wir wollen jetzt (104) beweisen. Es ist nach (101) und (52) offenbar

$$\lim_{t\to\infty} t^+ = 1 - \alpha S,$$

wobei

$$S = \sum_{e=0}^{\infty} \frac{1}{(2^1-1)(2^2-1)\cdots(2^e-1)\,2^e}$$

und in dieser Reihe als Anfangsglied (für $e = 0$) 1 zu verstehen ist. Dann ist

$$S = 1 + \frac{1}{2} + \sum_{e=2}^{\infty} \frac{1}{(2^1-1)(2^2-1)\cdots(2^e-1)} - \sum_{e=2}^{\infty} \frac{1}{(2^1-1)(2^2-1)\cdots(2^{e-1}-1)\,2^e}.$$

Die erste Summe geht, mit α multipliziert, nach (52) in

$$\lim_{t\to\infty} (t_2 + t_3 + \cdots + t_{t-1}) = \lim_{t\to\infty} (1 - t_0 - t_1) = 1 - 2\alpha$$

über. Die zweite Summe ist, mit 2 multipliziert, offenbar $S - 1$. Es ist also $S = 1 + \frac{1}{2} + \frac{1}{\alpha} - 2 - \frac{1}{2}S + \frac{1}{2}$, woraus $\alpha S = \frac{2}{3}$ folgt. Der obige Grenzwert ist also $1 - \alpha S = \frac{1}{3}$, und damit ist (104) bewiesen.

Die Behauptung $1^? < 3^? < 5^? < \cdots$ ist wegen (102) eine unmittelbare Folgerung aus 3. und 4. von Satz IV. Auch $2^? < 4^?$ ist nach der obigen Tabelle richtig. Für den Rest der Behauptung $4^? < 6^? < 8^? < \cdots$ genügt es wieder wegen (102) und 4. von Satz IV zu beweisen, daß die Summe $\frac{1}{4}t_1 + \frac{7}{32}t_2$ für $2 \mid t$ $(t \geqq 4)$ zunimmt, wenn t durch $t + 2$ ersetzt wird. Nun hat dieser Ausdruck in diesem Falle nach (58) den Wert

$$\frac{1}{4}t_1 + \frac{7}{32} \cdot \frac{1}{3}\left(1 - \frac{1}{2^{t-2}}\right)t_1 = \frac{1}{96}\left(31 - \frac{28}{2^t}\right)t_1.$$

Dies geht nach Einsetzen von $t + 2$ an Stelle von t wegen (57) über in:

$$\frac{1}{96}\left(31 - \frac{7}{2^t}\right)\left(1 - \frac{1}{2^{t+1}}\right)t_1.$$

Dies ist für $t \geqq 4$ in der Tat größer als der vorige Ausdruck, woraus die Behauptung folgt.

Da endlich (105) eine Folgerung aus (99), (103), (104) ist, ist der Satz X vollständig bewiesen.

14. Im Anschluß an Nagell [12]) bezeichne ich mit $B(x, t)$ und $C(x, t)$ die Anzahl derjenigen Zahlen $D \leqq x$, die aus genau t verschiedenen Primzahlfaktoren zusammengesetzt sind und für die die Norm der Grundeinheit negativ bzw. positiv ist. Die analogen Anzahlen sollen $B(x)$ und $C(x)$ bedeuten, wenn die Anzahl der Primfaktoren von D beliebig ist.

Offenbar ist mit ähnlichen Bezeichnungen wie in (96), (97)

(108) $$B(x, t) \geqq D(x, t, -), \quad C(x, t) \geqq D(x, t, +)$$

[12]) A. a. O. [4]).

und

$$B(x,t) + C(x,t) = D(x,t). \tag{109}$$

Daraus folgt offenbar

$$\frac{\frac{D(x,t,+)}{D(x,t)}}{1-\frac{D(x,t,+)}{D(x,t)}} \leqq \frac{C(x,t)}{B(x,t)} \leqq \frac{1-\frac{D(x,t,-)}{D(x,t)}}{\frac{D(x,t,-)}{D(x,t)}},$$

wenn x so groß ist, daß die Nenner nicht verschwinden. Nach (96), (97) und den Sätzen IX und X erhalten wir daraus den folgenden

Satz XI. *Es ist*

$$\frac{t^+}{1-t^+} \leqq \liminf_{x\to\infty} \frac{C(x,t)}{B(x,t)}, \quad \limsup_{x\to\infty} \frac{C(x,t)}{B(x,t)} \leqq \frac{1-t^-}{t^-},$$

wobei t^+, t^- durch Satz IX *gegeben sind.*

Die hier gegebenen Schranken $t' = \frac{t^+}{1-t^+}$, $t'' = \frac{1-t^-}{t^-}$ wachsen monoton mit t und streben den Werten $\frac{1}{2}$ bzw. $\frac{96-121\alpha}{121\alpha}$ zu, wobei α die Zahl in (53) *bedeutet. Es ist also*

$$0.5 \leqq \lim_{t\to\infty}\left(\liminf_{x\to\infty}\frac{C(x,t)}{B(x,t)}\right), \quad \lim_{t\to\infty}\left(\limsup_{x\to\infty}\frac{C(x,t)}{B(x,t)}\right) \leqq 0.891\ldots\left(=\frac{96-121\alpha}{121\alpha}\right).$$

(Einige Anfangswerte dieser Schranken t', t'' sind: $1' = 0, 1'' = 0$; $2' = 0.333\ldots, 2'' = 0.6$; $3' = 0.391\ldots, 3'' = 0.673\ldots$; $4' = 0.458\ldots, 4'' = 0.817\ldots$)

Es kommt also bei festem t öfter $n(\varepsilon) = -1$ als $n(\varepsilon) = +1$ vor, doch nie doppelt so oft, abgesehen vom Falle $t = 1$.

Dieser Satz läßt sich als Aussage über (untere und obere) relative Wahrscheinlichkeiten deuten, wie in der Einleitung bemerkt war.

Wie schon erwähnt, kann ich über $B(x)$ und $C(x)$ keine ähnlichen Aussagen gewinnen. Nur den folgenden Satz kann ich aussprechen, der wegen $B(x) \geqq B(x,t)$, $C(x) \geqq C(x,t)$ aus (108), (96), (97), dem Satz IX und aus (23) unmittelbar folgt:

Satz XII. *Für jedes positive t gilt bei genügend großem x mit von t abhängigen positiven Konstanten c_1, c_2*

$$B(x) > c_1 \frac{x(\log\log x)^t}{\log x}, \quad C(x) > c_2 \frac{x(\log\log x)^t}{\log x}.$$

Insbesondere ist diese sich auf $C(x)$ beziehende Abschätzung wesentlich besser als die bisher bekannten (vgl. Nagell, a. a. O. [4]), S. 4).

IV. Teil.

15. Die Betrachtungen über e_4 im II. Teil waren darauf gegründet, daß e_4 durch den quadratischen Typus T von D bestimmt ist. Nach der Arbeit R gibt es einen Zusammenhang zwischen e_8 und dem biquadratischen Typus U von D. Dieser Zusammenhang ist aber zu locker, um daraus ähnliche Schlüsse auf e_8 ziehen zu können. Während z. B. jede denkbare Kombination e_2, e_4 $(0 \leqq e_4 \leqq e_2)$, wie wir gesehen haben, unendlich oft vorkommt, kann ich nicht beweisen, daß jede Kombination e_2, e_4, e_8 $(0 \leqq e_8 \leqq e_4 \leqq e_2)$ möglich ist. Dagegen kann ich das unendlich oftmalige Auftreten eines jeden Tripels $e_2 \geqq 1, e_4 = 1, e_8 = 0, 1$ bestätigen. Wir hatten auch $M_t(e_4)$ genau angeben können. Demgegenüber sind wir jetzt nur in der Lage, für den ähnlichen Mittelwert $M_t(e_8)$, richtiger gesagt für den entsprechenden oberen und unteren Mittelwert $\overline{M}_t(e_8)$ und

$\underline{M}_t(e_8)$, eine obere und untere Schranke bestimmen zu können. So stellt man leicht fest, daß $\overline{M}_2(e_8) = M_2(e_8) = \frac{1}{8}$, $\overline{M}_3(e_8) \leqq \frac{11}{64}$ ist (dies ist mit $M_2(e_4) = \frac{1}{2}$, $M_3(e_4) = \frac{5}{8}$ zu vergleichen). Es scheint, daß im allgemeinen $\overline{M}_t(e_8)$ nicht wesentlich $\frac{1}{4} M_t(e_4)$ überschreitet. Da aber eine möglichst gute Abschätzung komplizierte Rechnungen erfordert, will ich mich damit hier nicht beschäftigen. Wohl aber kann man $\underline{M}_t(e_8)$ ziemlich gut und leicht nach unten abschätzen. Nach dieser Abschätzung ist — vorläufig nur grob gesagt — $\underline{M}_t(e_8) > \frac{1}{8} M_t(e_4)$ $(t \geqq 2)$.

Es gilt der folgende

Satz XIII. *Unter allen reell-quadratischen Körpern, deren Diskriminanten aus genau t $(t \geqq 2)$ verschiedenen positiven Primzahlen $\not\equiv 3 \pmod 4$ zusammengesetzt sind, haben die Fälle mit genau einer durch 8 teilbaren Invariante in der absoluten Klassengruppe des Körpers eine untere Wahrscheinlichkeit $\geqq \frac{1}{4} t_1$, wobei t_1 durch (51) gegeben ist. Zugleich ist also auch der untere Mittelwert $\underline{M}_t(e_8)$ der Anzahl dieser Invarianten $\geqq \frac{1}{4} t_1$.*

Unter den genannten Körpern haben nämlich die Fälle $e_4 = 1$ nach Satz II eine Wahrscheinlichkeit t_1. Diese Fälle umfassen die Diskriminanten, die zu gewissen quadratischen Typen T gehören. Zu jedem solchen T gibt es genau vier biquadratische Typen $U = (\alpha'_\Delta, \alpha''_\Delta)$, wobei $\Delta(\neq 1, D; D, 1)$ eine D-Zerfällung zweiter Art ist, die nach Satz V gleich wahrscheinlich sind. Da nach der Arbeit R, Satz II für $\alpha'_\Delta = \alpha''_\Delta = 1$, d. h. für $U = (1, 1)$, $e_8 = 1$ ist, folgt leicht die Richtigkeit des Satzes.

Ich will noch folgenden Satz erwähnen:

Satz XIV. *Unter entsprechenden Voraussetzungen wie im vorigen Satze, ist die obere Wahrscheinlichkeit dafür, daß alle geraden Invarianten der absoluten Klassengruppe sogar durch 8 teilbar sind, d. h. daß $e_8 = t - 1$ ist, $\leqq \frac{1}{2^{t^2-1}}$.*

Wenn nämlich $e_8 = t - 1$, dann ist zunächst $e_4 = t - 1$. Für das letztere ist die Wahrscheinlichkeit nach Satz II $t_{t-1} = \frac{1}{2^{\binom{t}{2}}}$. Wegen Satz I kommt jetzt offenbar nur ein einziger quadratischer Typus T in Frage (der also durchweg aus 1 besteht). Zu diesem T gibt es nach Satz V wegen $e_4 = t - 1$ genau $2^{\frac{(t-1)(t+2)}{2}}$ biquadratische Typen U, die alle gleich wahrscheinlich sind. Aus der Arbeit R, Satz IV folgt, daß im Falle $e_8 = t - 1$ notwendig U durchweg aus 1 besteht. Dieses einzige U hat nach dem Vorigen die Wahrscheinlich- keit $\frac{1}{2^{t^2-1}}$, womit der Satz bewiesen ist.

Eingegangen 12. April 1935.

Berichtigungen zu zwei früheren Arbeiten.

1. Ds. Journ. **171**, S. 137, Z. 10 soll $q \neq 2$ sein.
2. Ds. Journ. **173**, S. 195, Z. 13 soll $p \neq 2$ sein.

L. Rédei.

Über allgemeine Quadraturformeln.

Von *R. v. Mises* in Istanbul.

Kürzlich hat an dieser Stelle Herr R. Schmidt [1]) für den Satz, den Herr G. Kowalewski [2]) in seinem schönen Buch über Interpolation als „Newtonsche Quadraturformel" bezeichnet, eine neue Ableitung gegeben und eine Ausdehnung auf Stieltjessche Integrale hinzugefügt. Ich nehme dies zum Anlaß, um im folgenden darauf hinzuweisen, wie man auf ganz elementarem Wege eine weit umfassendere Gleichung gewinnen kann, die außer der Newtonschen Formel z. B. den Gaußschen Quadraturansatz, andrerseits auch die Eulersche Summenformel usf. als Spezialfälle enthält. Der Beweis erfordert nichts als die Kenntnis der Regel der partiellen Integration; von Approximation durch eine konvergente Folge von Integralen, wie sie in der Arbeit von Herrn R. Schmidt auftritt, oder dergleichen ist keine Rede.

Die Ausdehnung auf Stieltjessche Integrale bereitet nicht nur keinerlei Schwierigkeiten, sondern sie gestattet sogar, die Ableitung noch einfacher und übersichtlicher zu gestalten. Gleichwohl habe ich in § 1 den Fall gewöhnlicher Riemannscher Integrale vorangestellt [3]), um den elementaren Charakter des Problems auch nach dieser Richtung hin hervortreten zu lassen. Wer sich nur für das allgemeinste Problem interessiert, kann unmittelbar bei Satz 4 beginnen, der alles Frühere einschließt und für den eine von dem Vorangehenden unabhängige Ableitung gegeben ist.

Den tieferen Grund dafür, daß eine so weitgehende Zusammenfassung aller Quadratur- und Summenformeln gegeben werden konnte, wird man vielleicht darin finden, daß das Quadraturproblem hier völlig von dem der Interpolation losgelöst worden ist [4]), das sonst in der Regel den Zugang bildet. Auf einige spezielle Anwendungen und Erweiterungen der Theorie, insbesondere auf die *Abschätzungen* des Restgliedes, wird im folgenden nicht eingegangen.

§ 1. Verallgemeinerte Newtonsche Quadraturformel.

Wir untersuchen das bestimmte Integral $\int_a^b f\,dx$ in endlichen Grenzen und können ohne Beschränkung der Allgemeinheit 0 und 1 als Endpunkte des Integrationsintervalls wählen. Dagegen wollen wir die in der R. Schmidtschen Arbeit enthaltene Beschränkung, daß die Endpunkte des Intervalls stets zu den ausgezeichneten Punkten gehören, fallen lassen. Folgendes werden wir beweisen:

[1]) R. Schmidt, Dieses Journal **173** (1935), S. 52—59.

[2]) G. Kowalewski, Interpolation und genäherte Quadratur, Leipzig 1932, S. 73.

[3]) Das wesentliche Ergebnis von § 1, abgesehen von dem (leicht zu erbringenden) Eindeutigkeitsbeweis, findet sich schon in der Arbeit von W. Wirtinger, Zeitschr. f. angew. Math. u. Mech. **13** (1933), S. 166. Hier stützt sich die Ableitung auf die Integralform des Restgliedes der Taylorschen Formel und das Resultat wird in Zusammenhang gebracht mit der Fourier-Entwicklung der Bernoullischen Polynome. Die Ableitung des Textes benutzt dagegen nur die elementaren Regeln der partiellen Integration.

[4]) Diesem Gedankenkreis gehört auch meine Note „Zur mechanischen Quadratur" in Z. f. ang. Math. u. Mech. **13** (1933), S. 53—56 an.

Satz 1. *Es sei $f(x)$ im Intervall 0, 1 m-mal differenzierbar, $f^{(m)}(x)$ die m-te Ableitung und* [5])

$$0 = a_0 \leqq a_1 < a_2 < \cdots < a_n \leqq a_{n+1} = 1. \tag{1}$$

Wenn dann die n Konstanten $A_1, A_2, \ldots, A_n$ den m Gleichungen

$$\sum_{\nu=1}^{n} a_\nu^\mu A_\nu = \frac{1}{\mu+1}, \qquad \mu = 0, 1, 2, \ldots, m-1, \tag{2}$$

genügen und die m Funktionen $M_1(x), M_2(x), \ldots, M_m(x)$ im Intervall 0, 1 durch

$$M_{\mu+1}(x) = -\int_0^x M_\mu(\xi)\, d\xi, \qquad \mu = 1, 2, 3, \ldots, m-1 \tag{3}$$

$$M_1(x) = -x + A_1 + A_2 + \cdots + A_\nu \quad \text{für} \quad a_\nu < x < a_{\nu+1}; \quad \nu = 0, 1, 2, \ldots, n,$$

definiert sind, so gilt für $\mu = 1, 2, 3, \ldots, m$ identisch in f:

$$\int_0^1 f(x)\, dx = A_1 f(a_1) + A_2 f(a_2) + \cdots + A_n f(a_n) + \int_0^1 M_\mu(x)\, f^{(\mu)}(x)\, dx. \tag{4}$$

Die Definition (3) läßt die Werte von M_1 an den Stellen $a_1, a_2, \ldots, a_n$ unbestimmt, aber es existieren die beiden Grenzwerte bei Annäherung an a_ν von rechts und von links. In der üblichen Bezeichnungsweise hat man

$$M_1(a_\nu + 0) - M_1(a_\nu - 0) = A_\nu \tag{5}$$

für jeden im Innern gelegenen Punkt a_ν, also immer für $\nu = 2, 3, \ldots, n-1$ und für $\nu = 1$ und n, falls $a_1 > 0$ bzw. $a_n < 1$. In diesem Falle zeigt (3), daß $M_1(0) = 0$ und $M_1(1) = -1 + A_1 + A_2 + \cdots + A_n = 0$ zufolge der ersten Gl. (2). Ist aber $a_1 = 0$, so strebt $M_1(x)$, wenn man sich dem Wert $x = 0$ von rechts nähert, gegen A_1, und ebenso geht im Falle $a_n = 1$ der Wert von $M_1(x)$ bei Annäherung an $x = 1$ von links gegen $-1 + A_1 + A_2 + \cdots + A_{n-1} = -A_n$. Mithin kann man (5) für alle Fälle aufrechterhalten, wenn man bei $a_1 = 0$ für den noch nicht definierten Ausdruck $M_1(a_1 - 0)$ und ebenso bei $a_n = 1$ für $M_1(a_n + 0)$ den Wert 0 einsetzt.

Der Beweis des Satzes 1 erfolgt nunmehr in drei Schritten: Wir zeigen a) daß Gl. (4) bei $m \geqq 1$ für $\mu = 1$ gilt; hierauf leiten wir b) einen Hilfssatz ab, wonach $M_\mu(1) = 0$ für $\mu = 2, 3, \ldots, m$; endlich c) folgern wir aus a) und b), daß (4) für jeden Index $\mu \leqq m$ zu Recht besteht.

a) Durch Zerlegung des Intervalls in die Teile a_0 bis a_1, a_1 bis a_2 usf. und jedesmalige partielle Integration findet sich:

$$\int_0^1 M_1(x)\, f'(x)\, dx = \sum_{\nu=0}^{n} \int_{a_\nu}^{a_{\nu+1}} M_1(x)\, f'(x)\, dx$$

$$= \sum_{\nu=0}^{n} \Big[M_1(a_{\nu+1} - 0)\, f(a_{\nu+1}) - M_1(a_\nu + 0)\, f(a_\nu) - \int_{a_\nu}^{a_{\nu+1}} M_1'(x)\, f(x)\, dx \Big].$$

Da im Innern jedes Intervalls $M_1' = -1$ ist, so gibt der letzte Ausdruck rechts einfach $\int_0^1 f\, dx$. Die vorangehenden Glieder sind nach (5) und dem, was oben über das Verhalten von $M_1(x)$ bei $x = 0$ und $x = 1$ gesagt wurde, gleich $-\Sigma A_\nu f(a_\nu)$, so daß wir haben:

$$\int_0^1 M_1(x)\, f'(x)\, dx = -\sum_{\nu=1}^{n} A_\nu f(a_\nu) + \int_0^1 f(x)\, dx. \tag{6}$$

Dies ist nichts anderes als Gl. (4) für $\mu = 1$; dabei war von den Gl. (2) nur die erste, für $\mu = 0$, vorausgesetzt worden.

[5]) Der Fall, daß ein Teil der a_ν außerhalb des Integrationsintervalls liegt, wird in §§ 3 u. 4 bei Betrachtung der Stieltjes-Integrale miterledigt.

b) Die durch (3) definierten Funktionen $M_\mu(x)$ sind unmittelbar anzuschreiben:

$$(7)\quad M_\mu(x) = \frac{1}{\mu!}(-x)^\mu + \frac{1}{(\mu-1)!}[A_1(a_1-x)^{\mu-1} + A_2(a_2-x)^{\mu-1} + \cdots + A_\nu(a_\nu - x)^{\mu-1}]$$

für $a_\nu \leqq x \leqq a_{\nu+1}$ (Gleichheitszeichen nur bei $\mu \geqq 2$).

Die rechte Seite ist für $\mu \geqq 2$ eine stetige Funktion von x. Man überzeugt sich dann durch Differenzieren, daß die erste, und durch Einsetzen von $\mu = 1$, daß die zweite der Gl. (3) durch (7) befriedigt wird. Gl. (7) zeigt auch, daß $M_\mu(x)$ für $\mu \geqq 3$ durchweg $(\mu-2)$-mal differenzierbar ist. Schon aus der ersten Gl. (3) geht hervor, daß

$$(8)\qquad M_2(0) = M_3(0) = \cdots = M_m(0) = 0.$$

Die Bedingungsgleichungen (2) sind, wie man leicht sieht, äquivalent der Behauptung, daß für jedes Polynom von höchstens $(m-1)$-tem Grade

$$(9)\quad \sum_{\nu=1}^{n} P(a_\nu)\, A_\nu = \int_0^1 P(\xi)\, d\xi, \qquad P(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{m-1} x^{m-1}.$$

Denn einerseits folgen aus (9) mit $P(x) = x^\mu$ die Gl. (2), andrerseits geben diese Gleichungen, wenn man die erste mit c_0, die zweite mit $c_1, \ldots$, die letzte mit c_{m-1} multipliziert und addiert, genau Gl. (9).

Wählt man $P(\xi) = (\xi - 1)^{\mu-1}$, so gibt (9)

$$(10)\quad 0 = -\int_0^1 (\xi-1)^{\mu-1}\, d\xi + \sum_{\nu=1}^{n} A_\nu (a_\nu - 1)^{\mu-1} = \frac{1}{\mu}(-1)^\mu + \sum_{\nu=1}^{n} A_\nu (a_\nu - 1)^{\mu-1}.$$

Dieser Ausdruck unterscheidet sich nur durch den Faktor $(\mu-1)!$ von der rechten Seite von (7), wenn man darin x gegen 1 gehen läßt. Also ist (mit Rücksicht auf die Stetigkeit von M_μ für $\mu \geqq 2$)

$$(11)\qquad M_2(1) = M_3(1) = \cdots = M_m(1) = 0.$$

Dieses war zu zeigen. Nebenbei bemerkt, folgt aus (11), daß man die Gl. (3) auch durch

$$(12)\qquad M_{\mu+1}(x) = \int_x^1 M_\mu(\xi)\, d\xi, \qquad \mu = 1, 2, 3, \ldots, m-1,$$

$$M_1(x) = (1-x) - (A_n + A_{n-1} + \cdots + A_{\nu+1}) \quad \text{für} \quad a_\nu < x < a_{\nu+1}$$

ersetzen kann, woraus sich als zweiter Ausdruck für M_μ ergibt:

$$(13)\quad M_\mu(x) = \frac{1}{\mu!}(1-x)^\mu - \frac{1}{(\mu-1)!}[A_n(a_n - x)^{\mu-1} + A_{n-1}(a_{n-1} - x)^{\mu-1} + \cdots + A_{\nu+1}(a_{\nu+1} - x)^{\mu-1}]$$

für $a_\nu \leqq x \leqq a_{\nu+1}$ (Gleichheitszeichen nur bei $\mu \geqq 2$).

Die Gleichheit von (7) und (13) geht auch unmittelbar hervor aus der Anwendung von (9) auf das Polynom $P(\xi) = (\xi - x)^{\mu-1}$.

c) Oben unter a) war gezeigt worden, daß (4) für $\mu = 1$ zu Recht besteht. Um (4) für alle $\mu \leqq m$ sicherzustellen, muß man noch beweisen, daß für $\mu = 2, 3, \ldots, m$

$$(14)\qquad \int_0^1 M_1(x)\, f'(x)\, dx = \int_0^1 M_\mu(x)\, f^{(\mu)}(x)\, dx.$$

In der Tat liefert fortgesetzte partielle Intergation mit Rücksicht auf den eben abgeleiteten Hilfssatz (11) und auf (8):

$$\int_0^1 M_1 f'\,dx = -\,M_2 f'\Big|_0^1 + \int_0^1 M_2 f''\,dx = \int_0^1 M_2 f''\,dx = \cdots$$

$$= \int_0^1 M_{m-1} f^{(m-1)}\,dx = -\,M_m f^{(m-1)}\Big|_0^1 + \int_0^1 M_m f^{(m)}\,dx = \int_0^1 M_m f^{(m)}\,dx\,. \tag{15}$$

Damit ist Satz 1 bewiesen.

G. Kowalewski und nach ihm R. Schmidt legen großen Nachdruck auf die sogenannte Eindeutigkeit der Newtonschen Quadraturformel. In dem allgemeineren Fall unserer Formel (4) lautet die entsprechende Aussage wie folgt:

Satz 2. *Damit die Formel* (4) *für irgend ein* $\mu = m$ *identisch in* f *erfüllt sei, ist notwendig, daß die* A_ν *den Gl.* (2) *für* $\mu = 0, 1, 2, \ldots, m-1$ *genügen und daß* $M_m(x)$ *in jedem Stetigkeitspunkt mit der durch* (3) *bzw. durch* (7), (12) *oder* (13) *definierten Funktion übereinstimmt.*

Der erste Teil der Behauptung ist damit bewiesen, daß $f(x) = x^\varkappa$, mit ganzzahligem $\varkappa < m$, in (4) mit $\mu = m$ eingesetzt unmittelbar die Gl. (2) für $\mu = \varkappa$ ergibt. Nehmen wir nun an, es gäbe nach Verfügung über die A_ν eine Funktion $\bar{M}_m(x)$, die verschieden ist von der bereits bekannten $M_m(x)$ und in (4) eingesetzt werden darf, so müßte identisch in $f^{(m)}(x)$

$$\int_0^1 [\bar{M}_m(x) - M_m(x)]\, f^{(m)}(x)\,dx = 0 \tag{16}$$

sein. Ist aber $\bar{M}_m(x)$ in der Umgebung von $x = x_1$ stetig und $\bar{M}_m(x_1) \neq M_m(x_1)$, so gibt es ein Intervall α, β, das x_1 einschließt, aber keinen der Punkte a_ν (Unstetigkeitsstellen von M_1), und in dem $\bar{M}_m(x) - M_m(x)$ sein Zeichen nicht ändert. Wählt man dann $f^{(m)}(x)$ so, daß es außerhalb α, β verschwindet und im Innern des Intervalls positiv ist, so ist der Widerspruch mit (16) hergestellt.

Man kann Satz 1 und 2 auch in die Aussage zusammenfassen: *Damit eine Gleichung von der Form* (4) *identisch in* $f(x)$ *gilt, ist notwendig und hinreichend, daß sie für*

$$f(x) = 1,\quad x, x^2, \ldots, x^{m-1}$$

erfüllt ist; die Funktion $M_m(x)$ *ist nach Wahl der Koeffizienten* A_ν *im wesentlichen eindeutig bestimmt.*

§ 2. Spezielle Fälle.

a) *Newtonsche Quadratur*: *Fall* $m = n$. Wir gelangen zu der Newtonschen Quadraturformel, die ursprünglich aus dem Gedankenkreis der Interpolation hervorgegangen ist, indem wir in unserm allgemeinen Ansatz (4) $m = n$ setzen. Aus (2) wird ein System von n linearen Gleichungen mit n Unbekannten, dessen Determinante eine Vandermondesche ist, also wegen (1) nicht verschwindet. In der Formel (4) für $\mu = m = n$

$$\int_0^1 f(x)dx = A_1 f(a_1) + A_2 f(a_2) + \cdots + A_n f(a_n) + \int_0^1 M_n(x)\, f^{(n)}(x)\,dx \tag{17}$$

sind somit die Werte der A_ν durch (2) und infolgedessen die Funktion $M_n(x)$ durch (3) bzw. (7), (13) *eindeutig* bestimmt. Andrerseits besagt Satz 2, daß eine Erfüllung von (21) durch andere A_ν und M_n als die durch (2) und (3) definierten nicht möglich ist. Damit ist die „Eindeutigkeit" der Newtonschen Quadraturformel (21) bewiesen.

Die Identität unserer Konstanten A_ν mit den in der Interpolationstheorie gebräuchlichen geht unmittelbar daraus hervor, daß man aus (9) jedes einzelne A_ν berechnen kann, indem man für $P(\xi)$ das betreffende Lagrangesche Polynom einsetzt.

b) *Symmetrische Intervallteilung*: *Fall* $m = n + 1$. Setzt man in (9) für $P(\xi)$ der Reihe nach die steigenden Potenzen von $(\xi - \frac{1}{2})$, so erhält man als Ersatz für das Glei-

chungssystem (2):

$$(18)\qquad \sum_{\nu=1}^{n} A_\nu (a_\nu - \tfrac{1}{2})^\mu = 0 \qquad \text{für ungerade } \mu$$

$$= \frac{2^{-\mu}}{\mu+1} \qquad \text{für gerade } \mu.$$

Hieraus ersieht man: Wenn die a_ν symmetrisch zur Intervallmitte liegen, nämlich so, daß $a_1 = 1 - a_n$, $a_2 = 1 - a_{n-1}$, . . ., so werden die ersten n Gleichungen des Systems (18) oder, was dasselbe ist, des Systems (2) durch ein symmetrisches Wertsystem $A_1 = A_n$, $A_2 = A_{n-1}$, . . . befriedigt. Eine solche Lösung erfüllt aber *jede* der (unendlich vielen) Gleichungen (18) für ungerades μ. Ist daher n eine ungerade Zahl, so sind die Werte A_ν, die den Gl. (2) für $\mu = 0, 1, 2, \ldots, n-1$ genügen, auch eine Lösung der Gl. (2) für $\mu = 0, 1, 2, \ldots, n$, und man kann nach Satz 1 die Formel (4) für $\mu = n+1$ ansetzen. Damit sind wir zu dem von der Simpsonschen Regel her ($n = 3$) bekannten Resultat gelangt: *Bei ungeradem n und symmetrischer Anordnung der Teilpunkte a_ν gilt*

$$(19)\qquad \int_0^1 f(x)dx = A_1 f(a_1) + A_2 f(a_2) + \cdots + A_n f(a_n) + \int_0^1 M_{n+1}(x)\, f^{(n+1)}(x)dx.$$

Übrigens ist die Symmetrie der a_ν keine *notwendige* Bedingung für das Bestehen von (19), worauf wir noch unter f) zurückkommen werden.

c) *Gaußsche Quadratur: Fall $m = 2n$.* Wenn man die Abszissen der Teilpunkte a_ν nicht als von vornherein gegeben ansieht, sondern sie teilweise oder sämtlich als Unbekannte in die Gl. (2) eintreten läßt, so kann man *mehr* als n von den Gl. (2) befriedigen. Am bekanntesten ist der von Gauß behandelte Fall, in dem *alle* a_ν aus (2) bestimmt werden. Gauß hat gezeigt, daß diese Gleichungen mit $\mu = 0, 1, 2, \ldots, 2n-1$ eine eindeutige Lösung A_ν, a_ν ($\nu = 1, 2, \ldots, n$) besitzen, die den Bedingungen (1) genügt. Daher führt Satz 1 zu der Gleichung

$$(20)\qquad \int_0^1 f(x)dx = A_1 f(a_1) + A_2 f(a_2) + \cdots + A_n f(a_n) + \int_0^1 M_{2n}(x)\, f^{(2n)}(x)dx$$

für *diese* besondere Wahl der a_ν.

Ist z_μ die Anzahl der Zeichenwechsel von $M_\mu(x)$ im Intervall 0, 1, so folgt aus der ersten Gl. (3), daß

$$(21)\qquad z_{\mu-1} \geqq z_\mu + 1.$$

Sehen wir von dem Fall $a_1 = 0$ oder $a_n = 1$ ab, so hat $M_1(x)$ der Definition nach höchstens $2n-1$ Zeichenwechsel und $M_{m-1}(x)$ mindestens einen, weil $M_m(x)$ noch an beiden Enden verschwindet. Also gelten die Ungleichheiten

$$(22)\qquad m - \mu \leqq z_\mu \leqq 2n - \mu.$$

Daraus folgt für $\mu = m = 2n$, daß $M_{2n}(x)$ sein Zeichen im Intervall nicht ändert, was für die Fehlerabschätzung von (20) wichtig ist. Für beliebiges m gilt wegen (11)

$$(23)\qquad \int_0^1 M_m(x)\,dx = \int_0^1 x M_{m-1}(x)\,dx = \cdots = \frac{1}{(m-1)!}\int_0^1 x^{m-1} M_1(x)\,dx = \frac{1}{m!}\left[\frac{1}{m+1} - \sum_{\nu=1}^{n} a_\nu^m A_\nu\right].$$

Dies ist bei $m = 2n$ für das Fehlerglied in (20) maßgebend.

d) *Everetts Quadraturformeln.* Die in der Praxis viel verwendeten Formeln von Everett stellen ein Mittelding zwischen Quadratur- und Summenformel dar. Man geht aus von einer gleichförmigen Teilung des Intervalls in eine große Anzahl n von Teilen (wenn wir vorübergehend $n+1$ an Stelle des bisherigen n setzen), wobei der Mehrzahl der Funktionswerte der gleiche Koeffizient $A_\nu = \frac{1}{n}$ zugewiesen wird. Nur für die äußersten Ordinaten an den beiden Rändern (etwa die $k+1$ ersten und die $k+1$ letzten,

$2k < n-1$) variiert man die Werte von A_ν derart, daß eine kleine Anzahl der Gleichungen (2) befriedigt werden (wenn auch die übliche Begründung für die Bestimmung der Koeffizienten eine andere ist). Schreibt man f_ν für $f\left(\frac{\nu}{n}\right)$, so hat man den Ansatz

$$(24)\quad \int_0^1 f(x)\,dx = \frac{1}{n}\sum_{\nu=0}^{n} f_\nu + \frac{1}{n}\sum_{0}^{k} \alpha_\varkappa (f_\varkappa + f_{n-\varkappa}) + \int_0^1 M_m(x)\, f^{(m)}(x)\,dx\,.$$

Für die Formel vierter Ordnung, d. h. $m = 4$, wird angegeben [6])

$$k = 3; \quad \alpha_0 = -\frac{16}{24}, \quad \alpha_1 = \frac{7}{24}, \quad \alpha_2 = -\frac{4}{24}, \quad \alpha_3 = \frac{1}{24}.$$

Das zugehörige M_4 ist nach § 1 leicht zu bestimmen. Aber man kann, von der neuen Begründung ausgehend, auch eine einfachere Lösung für $m = 4$, nämlich mit $k = 2$, finden:

$$\alpha_0 = -\frac{15}{24}, \quad \alpha_1 = \frac{4}{24}, \quad \alpha_2 = -\frac{1}{24}.$$

Allgemein ist $k = m-2$ möglich (m gerade), während die bekannten Ansätze $k = m-1$ aufweisen. Die Gleichungen, denen die $\alpha_\varkappa$ vermöge (2) genügen müssen, sind

$$(25)\quad \Sigma\alpha_\varkappa = -\frac{1}{2}, \quad \Sigma\varkappa\alpha_\varkappa = \frac{1}{2}B_2, \quad \Sigma\varkappa^2\alpha = 0, \quad \Sigma\varkappa^3\alpha_\varkappa = -\frac{1}{4}B_4, \ldots,$$

wobei $B_2, B_4, \ldots$ die Bernoullischen Zahlen bedeuten.

e) *Methode von Tchebycheff.* Hier wird, wie bekannt, die Frage so gestellt: Wie muß man die ausgezeichneten Punkte a_ν wählen, wenn alle Koeffizienten A_ν einander gleich sein sollen? Die Bedingungsgleichungen, die Tchebycheff verwendet, sind identisch mit unseren Gl. (2). Daher liefert unsere Gl. (3) mühelos einen Ausdruck für den Rest.

Folgende Erweiterung des Verfahrens läßt sich jetzt leicht durchführen. Man nimmt eine Reihe von Abszissen willkürlich an, indem man sich nach der gegebenen Funktion richtet, immer mit den gleichen A_ν, und bestimmt nur den übrigen Teil aus den Gl. (2). Immer wenn man m Gleichungen berücksichtigt hat, ist das Fehlerglied von m-ter Ordnung angebbar. Die gesuchten Abszissen ergeben sich, genau wie in dem ursprünglich betrachteten Fall, als die Wurzeln einer Gleichung m-ten Grades, deren Koeffizienten mit Hilfe der Gl. (2) sich leicht bilden lassen.

f) *Erweiterung des Gaußschen Verfahrens.* Auch bei Verwendung des Gaußschen Quadraturgedankens erscheint es oft vorteilhaft, einen Teil der Abszissen, der besonderen Problemlage entsprechend, willkürlich anzunehmen und nur die übrigen, etwa in der Anzahl z, durch die Gl. (2) zu bestimmen. Das Fehlerglied von der Ordnung $n+z$ wird unmittelbar durch (3) geliefert.

Zur Berechnung der z unbekannten Abszissen kann man in folgender Weise aus $m = n+z$ Gleichungen (2) die n Koeffizienten A_ν eliminieren. Man setzt

$$(26)\qquad \omega(x) = (x-a_1)(x-a_2)\cdots(x-a_n)$$

und beachtet, daß der Ansatz (2) auf die Forderung (9) für ein beliebiges Polynom P vom Grad $n+z-1$ hinausläuft. Setzt man also der Reihe nach $\omega(x)$, $x\omega(x)$, ..., $x^{\alpha-1}\omega(x)$ für P ein, wobei die linke Seite wegen $\omega(a_\nu) = 0$ verschwindet, so hat man z Gleichungen für die z unbekannten a_ν allein. Sämtliche Koeffizienten A_ν berechnen sich dann als Integrale über die zu den a_ν gehörigen Lagrangeschen Polynome. Beispielsweise ist für $z = 1$, d. h. wenn man den Grad der Approximation nur auf $m = n+1$ erhöhen will, die einzige Bedingung die, daß $\int_0^1 \omega(x)\,dx = 0$. Dies ist die Verallgemeinerung des unter b) besprochenen Falles symmetrischer Abszissen.

[6]) Vgl. J. O. Irwin, On quadrature and cubature. Tracts for computers, ed. by Karl Pearson, No. X, Cambridge 1923, S. 14.

g) *Verwendung von Ableitungswerten.* Soll der Wert der ersten Ableitung $f'(x)$ der gegebenen Funktion an einer Stelle $x = a_\nu$ zur Berechnung des Integrals verwendet werden, so kann man unsere Formeln (2) und (3) unter Heranziehung eines Grenzübergangs benutzen. Wir gehen davon aus, daß die Funktionswerte in a_ν und $a_\nu + \delta$ gegeben seien und in der Schlußformel (4) mit den Koeffizienten $-B_\nu : \delta$ und $+B_\nu : \delta$ versehen werden sollen. Dann tritt in Gl. (2) an Stelle von $A_\nu a_\nu^\mu$

$$\frac{1}{\delta} B_\nu [(a_\nu + \delta)^\mu - a_\nu^\mu] \to \mu B_\nu a_\nu^{\mu-1} \tag{27}$$

ein und in den Ausdruck (7) für $M_\mu(x)$, von $x = a_\nu$ an,

$$\frac{1}{\delta} B_\nu \frac{1}{(\mu-1)!} [(a_\nu + \delta - x)^{\mu-1} - (a_\nu - x)^{\mu-1}] \to \frac{B_\nu}{(\mu-2)!} (a_\nu - x)^{\mu-2}. \tag{28}$$

Damit sind alle Fragen, auch hinsichtlich der höheren Ableitungen, grundsätzlich erledigt und man könnte z. B. das Restglied der Eulerschen Summenformel darnach hinschreiben. Wir werden jedoch weiter unten in § 4 die fertigen Ausdrücke für den Fall der Verwendung beliebiger Ableitungen angeben (Satz 4).

§ 3. Stieltjessche Integrale.

Wir betrachten jetzt Integrale der Form $\int_a^b f\, dV(x)$, worin V eine Funktion von beschränkter Schwankung bedeutet. Die Intervallgrenzen a, b normieren wir nicht, um den Übergang zu unendlichem Integrationsbereich nicht auszuschließen. Wir formulieren den dem § 1 analogen Satz, gleich unter Einschluß der „Eindeutigkeit", wie folgt.

Satz 3. *Es sei $f(x)$ im Intervall a, b m-mal differenzierbar, $f^{(m)}(x)$ die m-te Ableitung, $M_1(x)$ von beschränkter Schwankung und*

$$M_1(a) = 0. \tag{1}$$

Dann und nur dann, wenn $M_1(x)$ den m Bedingungen

$$\int_a^b x^\mu\, dM_1(x) = 0, \qquad \mu = 0, 1, 2, \ldots, m-1 \tag{2}$$

genügt und die $M_\mu(x)$ durch

$$M_{\mu+1}(x) = -\int_a^x M_\mu(\xi)\, d\xi, \qquad \mu = 1, 2, 3, \ldots, m-1 \tag{3}$$

definiert sind, gilt für $\mu = 1, 2, 3, \ldots, m$ identisch in f

$$\int_a^b f(x)\, dM_1(x) + \int_a^b M_\mu(x)\, f^{(\mu)}(x)\, dx = 0. \tag{4}$$

Wir beweisen zunächst, daß (1) bis (3) *hinreichende* Bedingungen für (4) sind, und zwar in denselben drei Schritten wie in § 1.

a) Aus (1) und der ersten Gl. (2) folgt, daß $M_1(a) = M_1(b) = 0$. Daher liefert partielle Integration

$$\int_a^b f(x)\, dM_1(x) = f\, M_1 \Big|_a^b - \int_a^b M_1(x)\, f'(x)\, dx = -\int_a^b M_1(x)\, f'(x)\, dx. \tag{5}$$

Damit ist (4) für $\mu = 1$ bewiesen.

b) Der explizite Ausdruck für $M_\mu(x)$ für $\mu \geqq 2$ lautet nach (3)

$$M_\mu(x) = \frac{1}{(\mu-1)!} \int_a^x (\xi - x)^{\mu-1}\, dM_1(\xi), \tag{6}$$

wie man durch Differentiation nach x feststellt; M_μ ist stetig für $\mu \geqq 2$ und von $\mu = 3$ an

mindestens $(\mu-2)$ mal differenzierbar. Die Gl. (2) besagen wieder, daß für jedes Polynom $P(\xi)$ von höchstens $(m-1)$-ten Grad

$$\int_a^b P(\xi)\, dM_1(\xi) = 0. \tag{7}$$

Setzt man hier $P(\xi) = (\xi - b)^{\mu-1}$ ein, so erhält man links, vom Faktor $(\mu-1)!$ abgesehen, den Ausdruck für $M_\mu(b)$ nach (6). Also ist bewiesen, daß

$$M_2(b) = M_3(b) = \cdots = M_m(b) = 0. \tag{8}$$

c) Aus (8) gewinnt man durch fortgesetzte partielle Integration

$$\begin{aligned}\int_a^b M_1 f'\,dx &= -M_2 f' \Big|_a^b + \int_a^b M_2 f''\,dx = \int_a^b M_2 f''\,dx = \cdots \\ &= \int_a^b M_{m-1} f^{(m-1)}\,dx = -M_m f^{(m-1)} \Big|_a^b + \int_a^b M_m f^{(m)}\,dx = \int_a^b M_m f^{(m)}\,dx .\end{aligned} \tag{9}$$

Wenn dies rechts in (5) eingesetzt wird, ist (4) in vollem Umfang bewiesen.

Daß umgekehrt für Gl. (4) bei $\mu = m$, also für

$$\int_a^b f(x)\, dM_1(x) + \int_a^b M_m(x)\, f^{(m)}(x)\, dx = 0 \tag{10}$$

die Bedingungen (2), (3) *notwendig* sind, sieht man so ein. Zunächst folgen aus (10), wenn man für $f(x)$ der Reihe nach $1, x, x^2, \ldots, x^{m-1}$ setzt, die Gl. (2). Hat man nun ein $M_1(x)$, das diesen Gl. (2) genügt, so ist durch (3) $M_m(x)$ eindeutig bestimmt. Gäbe es ein davon verschiedenes $\bar{M}_m(x)$, das (10) befriedigt, so müßte wieder Gl. (16) von § 1 identisch in $f^{(m)}(x)$ erfüllt sein, was aber nur dann möglich ist, wenn $\bar{M}_m$ an allen Stetigkeitsstellen mit M_m übereinstimmt.

Die *Anwendung* der Gl. (4) auf die Aufgaben der mechanischen Quadratur geschieht in folgender Weise: Ist eine Funktion von beschränkter Schwankung $V(x)$ mit $V(a) = 0$ gegeben und $\int f(x)\, dV(x)$ gesucht, so kann man z. B.

$$M_1(x) = -V(x) + A_1 + A_2 + \cdots + A_\nu, \text{ für } a_\nu < x < a_{\nu+1} \tag{11}$$
$$a = a_0 < a_1 < a_2 < \cdots < a_n < a_{n+1} = b$$

setzen. (Hierbei ist es keine Beschränkung der Allgemeinheit, daß wir die a_ν als im Innern des Intervalls a, b gelegen voraussetzen, vgl. § 4, S. 64.)

Das Differential $dM_1(x)$ setzt sich zusammen aus $-dV(x)$ und den Sprüngen $A_1, A_2, A_3, \ldots$ an den ausgezeichneten Stellen $a_1, a_2, a_3, \ldots$ Die Gl. (2) lauten daher für dieses $M_1(x)$

$$\sum_{\nu=1}^{n} A_\nu a_\nu^\mu = \int_a^b x^\mu dV(x), \qquad \mu = 0, 1, 2, \ldots, m-1, \tag{12}$$

und die zugehörigen $M_\mu(x)$ sind nach (6) durch

$$\begin{aligned}M_\mu(x) = \frac{1}{(\mu-1)!}\Big[-\int_a^x (\xi - x)^{\mu-1}\, dV(\xi) + A_1(a_1 - x)^{\mu-1} \\ + A_2(a_2 - x)^{\mu-1} + \cdots + A_\nu(a_\nu - x)^{\mu-1}\Big] \text{ für } a_\nu \leqq x \leqq a_{\nu+1}\end{aligned} \tag{13}$$

bestimmt. Die Gl. (4) nehmen die Form an $(\mu = 1, 2, 3, \ldots, m)$

$$\int_a^b f(x) dV(x) = A_1 f(a_1) + A_2 f(a_2) + \cdots + A_n f(a_n) + \int_a^b M_\mu(x)\, f^{(\mu)}(x)\, dx , \tag{14}$$

die sie unmittelbar als Quadraturformeln erkennen läßt.

Aber man kann auch vielfach verallgemeinerte Formeln aus (4) gewinnen, z. B. die von R. Schmidt abgeleitete, die neben den Funktionswerten $f(a_\nu)$ die einzelnen,

über die Teilintervalle erstreckten Integrale $\int_{a_\nu}^{a_{\nu+1}} f\,dx$ benutzt. Dazu ist nur notwendig, $n+1$ neue Konstante $B_0, B_1, B_2, \ldots, B_n$ einzuführen und M_1 so zu wählen, daß im Intervall a_ν bis $a_{\nu+1}$ das Differential $dM_1 = -dV + B_\nu dx$ wird, während der Sprung A_ν an der Stelle a_ν erhalten bleibt, also

$$(15)\quad M_1(x) = -V(x) + \sum_{\varkappa=1}^{\nu} [A_\varkappa + B_{\varkappa-1}(a_\varkappa - a_{\varkappa-1})] + B_\nu(x - a_\nu) \qquad \text{für } a_\nu < x < a_{\nu+1}.$$

Das weitere ist alles zwangläufig. Aus den Gl. (2) wird

$$(16)\quad \sum_{\nu=1}^{n} A_\nu a_\nu^\mu + \frac{1}{\mu+1}\sum_{\nu=0}^{n} B_\nu(a_{\nu+1}^{\mu+1} - a_\nu^{\mu+1}) = \int_a^b x^\mu dV(x), \quad \mu = 0, 1, 2, \ldots m-1,$$

die Quadraturformeln für $\mu = 1, 2, \ldots m$ lauten:

$$(17)\quad \int_a^b f(x)\,dV(x) = A_1 f(a_1) + \cdots + A_n f(a_n) + B_0 \int_{a_1}^{a_2} f(x)\,dx + \cdots + B_n \int_{a_n}^{b} f(x)\,dx + \int_a^b M_\mu(x) f^{(\mu)}(x)\,dx,$$

und der hier einzusetzende Ausdruck für $M_\mu(x)$ ist

$$(18)\quad M_\mu(x) = \frac{1}{(\mu-1)!}\left\{-\int_0^x (\xi - x)^{\mu-1} dV(\xi) + \sum_{\varkappa=1}^{\nu} [A_\varkappa + B_{\varkappa-1}(a_\varkappa - a_{\varkappa-1})](a_\varkappa - x)^{\mu-1} - \frac{B_\nu}{\mu}(a_\nu - x)^\mu\right\} \quad \text{für } a_\nu \leqq x \leqq a_{\nu+1}.$$

Dabei kann man $m \leqq 2n+1$ noch frei wählen, indem man bei der Wahl der A_ν und B_ν eine größere oder geringere Zahl der Gl. (16) berücksichtigt.

§ 4. Allgemeinster Ansatz.

Die Quadraturformel allgemeinster Art, die z. B. auch die Eulersche Summenformel umfaßt, erhalten wir, wenn wir annehmen, daß außer Funktionswerten $f(a_\nu)$ auch Werte der ϱ-ten Ableitungen an den Stellen $a_{\varrho\nu}$ ($\nu = 1, 2, 3, \ldots, n_\varrho$) herangezogen werden. Indem wir f selbst auch mit $f^{(0)}$ bezeichnen, haben wir also die Differenz

$$\int_a^b f(x)\,dV(x) - \sum_{\varrho,\nu} A_{\varrho\nu} f^{(\varrho)}(a_{\varrho\nu}), \qquad \varrho = 0, 1, 2, \ldots, r;\ \nu = 1, 2, 3, \ldots, n_\varrho,$$

zu untersuchen. Der Fall (der im letzten Beispiel vorlag), daß auch Integrale über Teilintervalle $\int_{\alpha_\nu}^{\beta_\nu} f\,dx$ benutzt werden, ist hier schon eingeschlossen. Man braucht nur in allen Formeln $V(x)$ durch $V(x) - W(x)$ zu ersetzen, wo $W(x)$ die Funktion bedeutet, die in den Intervallen α_ν, β_ν die Steigung B_ν besitzt und sonst konstant verläuft. (Diese Teilintervalle dürfen sich auch überdecken und man kann in den zugehörigen Integralen auch jeweils dx durch eine gegebene Funktion $dV_\nu(x)$ ersetzen.) Die B_ν gehen auf diese Weise in alle Gleichungen ein, die $V(x)$ enthalten. Da von $V(x)$ nur Beschränktheit der Schwankung gefordert wird, braucht auf $W(x)$ nicht weiter Rücksicht genommen zu werden.

Von den $a_{\varrho\nu}$ dürfen wir annehmen, daß sie sämtlich in das Innere von a, b fallen. Denn man kann stets, ohne den Wert des Integrals zu ändern, dem eigentlichen Integrationsgebiet an beiden Seiten beliebige Stücke hinzufügen, in denen man $V(x)$ konstant verlaufen läßt.

Wir formulieren nunmehr:

Satz 4. *Sei $f(x)$ im Intervall a, b m-mal differenzierbar, $f^{(\varrho)}$ die ϱ-te Ableitung, $f^{(0)} = f$, ferner $V(x)$ von beschränkter Schwankung und*

$$(1) \qquad a < a_{\varrho\nu} < b; \qquad \varrho = 0, 1, 2, \ldots, r < m; \quad \nu = 1, 2, 3, \ldots, n_\varrho.$$

Wenn dann die Koeffizienten $A_{\varrho\nu}$ den m Gleichungen

$$(2) \qquad \int_a^b x^\mu \, dV(x) = \sum_{\varrho \leqq \mu}{}' A_{\varrho\nu} \frac{\mu!}{(\mu - \varrho)!} a_{\varrho\nu}^{\mu-\varrho}, \quad \mu = 0, 1, 2, \ldots, m-1,$$

genügen, wobei Σ' über alle Wertverbindungen ϱ, ν bei $\varrho \leqq \mu$ erstreckt wird, und wenn die Funktionen $M_\mu(x)$ für $\mu > r$ durch

$$(3) \quad M_\mu(x) = -\frac{1}{(\mu-1)!} \int_a^x (\xi - x)^{\mu-1} \, dV(\xi) + \sum_{a_{\varrho\nu} < x}{}^* A_{\varrho\nu} \frac{(a_{\varrho\nu} - x)^{\mu-\varrho-1}}{(\mu - \varrho - 1)!}$$

definiert sind, wo Σ^* alle die Wertsysteme ϱ, ν zusammenfaßt, für die $a_{\varrho\nu} < x$ ist, so gilt identisch in $f(x)$ **für** *$\mu = r+1, r+2, \ldots, m$,*

$$(4) \qquad \int_a^b f(x) \, dV(x) - \sum_{\varrho,\nu} A_{\varrho\nu} f^{(\varrho)}(a_{\varrho\nu}) = \int_a^b M_\mu(x) \, f^{(\mu)}(x) \, dx,$$

die Summe Σ über sämtliche ϱ, ν genommen.

Umgekehrt müssen die Gl. (2) erfüllt sein, wenn (4) für $\mu = m$ identisch in f bestehen soll, und die in (4) auftretende Funktion $M_\mu(x)$ kann sich an keiner Stetigkeitsstelle von der in (3) definierten unterscheiden.

Wir stellen zunächst die folgenden Eigenschaften der durch (3) definierten Funktionen $M_\mu(x)$ fest:

1) Von den Punkten $a_{\varrho\nu}$ abgesehen ist $M_\mu(x)$ wenigstens $(\mu - 1)$-mal differenzierbar und die erste Ableitung von $M_\mu(x)$ stimmt mit dem Ausdruck für $-M_{\mu-1}(x)$ überein $(\mu > r+1)$. Ferner ist $M_\mu(a) = 0$ und für $\mu > r+1$ ist M_μ *überall* stetig, weil dann unter dem Summenzeichen keine nullten Potenzen von $(a_{\varrho\nu} - x)$ auftreten. Also gilt

$$(5) \qquad M_{\mu+1}(x) = -\int_a^x M_\mu(\xi) \, d\xi, \qquad \mu = r+1, r+2, \ldots, m.$$

2) Die Funktion $M_{r+1}(x)$ hat an den Stellen $x = a_{r\nu}$ $(\nu = 1, 2, 3, \ldots, n_r)$ Sprünge von der Größe $A_{r\nu}$. Läßt man die Glieder, die von $\varrho = r$ herrühren, im Ausdruck (3) fort, so bleibt eine stetige Funktion übrig, die das negative Integral einer neuen Funktion bildet, die aus (3) hervorgeht, wenn man hier $\mu = r$ setzt *und die Glieder mit $A_{r\nu}$ streicht.* Diese neue Funktion heiße $M_r(x)$; sie hat an den Stellen $a_{r-1,\nu}$ $(\nu = 1, 2, 3, \ldots, n_{r-1})$ Unstetigkeiten von der Größe $A_{r-1,\nu}$. Läßt man wieder diese Glieder fort, so bleibt das negative Integral einer Funktion $M_{r-1}(x)$ übrig, die an den Stellen $x = a_{r-2,\nu}$ Sprünge der Größe $A_{r-2,\nu}$ besitzt, usf. So wird eine Folge von Funktionen $M_1(x), M_2(x), \ldots, M_r(x)$ definiert, deren erste gegeben sind durch:

$$(6) \quad \begin{aligned} M_1(x) &= -\int_a^x dV(\xi) + \sum_\nu{}^* A_{0\nu} \\ M_2(x) &= -\int_a^x (\xi - x) \, dV(\xi) + \sum_\nu{}^* [A_{0\nu}(a_{0\nu} - x) + A_{1\nu}] \\ M_3(x) &= -\int_a^x \frac{1}{2} (\xi - x)^2 \, dV(\xi) + \sum_\nu{}^* \left[A_{0\nu} \frac{(a_{0\nu} - x)^2}{2} + A_{1\nu}(a_{1\nu} - x) + A_{2\nu} \right] \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Überall sind in Σ^* nur diejenigen ν zu berücksichtigen, für die $a_{\varrho\nu} < x$ ist. Man kann statt (6) auch unmittelbar die Gl. (3) für $\mu = 1, 2, \ldots r$ benützen, wenn man festsetzt, daß dort

die Summen nur über diejenigen Wertepaare ϱ, ν erstreckt werden sollen für die einerseits $a_{\varrho\nu} < x$, andrerseits $\varrho \leqq \mu - 1$.

Für alle diese Funktionen mit Einschluß der früher definierten $M_{r+1}(x)$, $M_{r+2}(x), \ldots$ gilt

$$M_\mu(x) = -\frac{dM_{\mu+1}(x)}{dx} \quad \text{für} \quad x \neq a_{\varrho\nu}, \qquad \mu = 1, 2, 3, \ldots, m-1. \tag{7}$$

Im Punkt $x = a_{\varrho\nu}$ hat allein $M_{\varrho+1}$ einen Sprung, und zwar von der Größe $A_{\varrho\nu}$.

3) Am unteren Intervallende $x = a$ haben alle $M_\mu(x)$ den Wert 0. Von dem oberen Endpunkt b wissen wir, daß er mit keinem der $a_{\varrho\nu}$ zusammenfällt. Sind aber alle $a_{\varrho\nu} < b$, so erhält man $M_\mu(b)$, indem man in (3) bzw. (6) $x = b$ einführt und dabei Σ^* durch Σ'', nämlich durch die über *alle* ν bei $\varrho \leqq \mu - 1$ erstreckten Summen ersetzt. Andrerseits besagt (2), daß für jedes Polynom $P(\xi)$ von höchstens $(m-1)$-tem Grad

$$-\int_a^b P(\xi)\, dV(\xi) + \Sigma' A_{\varrho\nu} P^{(\varrho)}(a_{\varrho\nu}) = 0. \tag{8}$$

Führt man $P(\xi) = (\xi - b)^{\mu-1}$ ein, so kann man Σ' durch Σ'' ersetzen, weil die μ-te Ableitung von $P(\xi)$ ohnehin verschwindet. Somit geht die linke Seite von (8) bis auf den Faktor $(\mu-1)!$ in die Ausdrücke für $M_\mu(b)$ über. Also ist

$$M_\mu(a) = M_\mu(b) = 0 \quad \text{für} \quad \mu = 1, 2, 3, \ldots, m. \tag{9}$$

Nunmehr ist die Ableitung der Formel (4) aus (2) und (3) ohne weiteres möglich. Zerlegt man das Intervall a, b in die durch die $a_{\varrho\nu}$ bestimmten Abschnitte und wendet für jeden einzelnen wiederholte partielle Integration an, so erhält man im Hinblick auf (7)

$$\int_\alpha^\beta M_\mu f^{(\mu)} dx = M_\mu f^{(\mu-1)}\Big|_\alpha^\beta + M_{\mu-1} f^{(\mu-2)}\Big|_\alpha^\beta + \cdots + M_2 f'\Big|_\alpha^\beta + M_1 f\Big|_\alpha^\beta - \int_\alpha^\beta f\, dM_1. \tag{10}$$

Bei der Summation über alle Teilintervalle fallen diejenigen $M_\varkappa$, die stetig sind, mit Rücksicht auf (9) heraus, d. s. die mit $\varkappa > r+1$. Dagegen führt z. B. $M_2 f'\Big|_\alpha^\beta$, da $M_2(x)$ an den Stellen $a_{1\nu}$ die Sprünge $A_{1\nu}$ aufweist, zu dem Ausdruck $-\Sigma A_{1\nu} f'(a_{1\nu})$, ebenso das Glied $M_3 f''\Big|_\alpha^\beta$ zur Summe $-\Sigma A_{2\nu} f''(a_{2\nu})$ usf. bis einschließlich $M_{r+1} f^{(r)}\Big|_\alpha^\beta$ mit dem Ergebnis $-\Sigma A_{r\nu} f^{(r)}(a_{r\nu})$. In dem Integral, das rechts in (10) steht, ist, da es sich nur auf das Innere eines Intervalls bezieht, das keinen der Punkte $a_{\varrho\nu}$ enthält, dM_1 durch $-dV$ zu ersetzen. So ergibt schließlich (10) nach Summierung über alle Teilintervalle

$$\int_a^b M_\mu(x)\, f^{(\mu)}(x)\, dx = -\sum_{\nu=1}^{n_0} A_{0\nu} f(a_{0\nu}) - \sum_{\nu=1}^{n_1} A_{1\nu} f'(a_{1\nu}) - \cdots - \sum_{\nu=1}^{n_r} A_{r\nu} f^{(r)}(a_{r\nu}) + \int_a^b f(x)\, dV(x),$$

und dies ist identisch mit Gl. (4).

Was nun den zweiten Teil des Satzes angeht, so sieht man sofort, daß die Gl. (2) aus (4) mit $\mu = m$ folgen, wenn man hier die Potenzen $1, x, x^2, \ldots, x^{m-1}$ für $f(x)$ einsetzt. Also ist notwendig, daß die Gl. (2) erfüllt sind. Hat man aber einmal die $A_{\varrho\nu}$ als eine Lösung der Gl. (2) gewählt, so ist $M_m(x)$ durch (3) eindeutig bestimmt. Gäbe es noch eine andere Funktion $\overline{M}_m(x)$, die (4) befriedigt, so müßte identisch in $f^{(m)}$

$$\int_a^b [\overline{M}_m(x) - M_m(x)]\, f^{(m)}(x)\, dx = 0 \tag{11}$$

sein, was nicht möglich ist, wenn $\overline{M}_m - M_m$ an einer Stelle, wo beide Funktionen stetig sind, nicht verschwindet.

Damit ist Satz 4 bewiesen. Man kann seinen wesentlichen Inhalt auch so aussprechen: *Bedeutet $L\{f\}$ irgendeine lineare Kombination von Funktionswerten und Werten der Ableitungen bis zur r-ten Ordnung von f, so ist die notwendige und hinreichende Bedingung dafür, daß bei $m > r+1$*

$$\int_a^b f\,dV = L\{f\} + \int_a^b M_m f^{(m)}\,dx \tag{12}$$

identisch in f mit stetigem M_m besteht, die, daß die Gleichung für jedes Polynom von höchstens $(m-1)$-tem Grad erfüllt ist; die Funktion M_m ist dann eindeutig durch die Koeffizienten von L nach (3) bestimmt.

Als Beispiel sei nur die *Eulersche Formel* angeführt, die, in leichter Abänderung der bisherigen Bezeichnung, so geschrieben werden kann:

$$\begin{aligned}\int_0^n f(x)\,dx = \sum_{\nu=0}^{n} f(\nu) + A_0[f(0)+f(n)] + A_1[f'(n)-f'(0)] + A_2[f'''(n)-f'''(0)] \\ + \cdots + A_m[f^{(2m-1)}(n) - f^{(2m-1)}(0)] + \int_0^n M_{2m+2}(x)\, f^{(2m+2)}\,dx\,.\end{aligned} \tag{13}$$

Hier sind die Gl. (2) für ungerade μ der Symmetrie wegen schon erfüllt, die übrigen lauten, wenn mit S_μ die Summe der μ-ten Potenzen der Zahlen 1 bis n bezeichnet wird,

$$\begin{aligned} n-(n+1) &= 2A_0 \\ \frac{n^3}{3} - S_2 &= A_0 n^2 + 2A_1 n \\ \frac{n^5}{5} - S_4 &= A_0 n^4 + 4A_1 n^3 + 4\cdot 3\cdot 2\, A_2 n \end{aligned} \tag{14}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\frac{n^{2m+1}}{2m+1} - S_{2m} = A_0 n^{2m} + 2m\,A_1 n^{2m-1} + 2m(2m-1)(2m-2)\,A_2 n^{2m-3} + \cdots + (2m)!\,A_m n.$$

Das zugehörige M_{2m+2} ist nach (3) gegeben durch

$$M_{2m+2}(x) = \frac{x^{2m+2}}{(2m+2)!} - (1+A_0)\frac{x^{2m+1}}{(2m+1)!} - \sum_{\varkappa=1}^{m} A_\varkappa \frac{x^{2m+2-2\varkappa}}{(2m+2-2\varkappa)!} + \sum_{\varkappa=1}^{\nu}\frac{(\varkappa-x)^{2m+1}}{(2m+1)!} \tag{15}$$

$$\text{für} \quad \nu \leqq x \leqq \nu+1.$$

Die Gleichungen (14) führen natürlich zu den bekannten Bernoullischen Zahlen. Aber an (13) ist bemerkenswert, daß das Restglied die Ordnung $2m+2$ hat, während die meisten üblichen Ableitungen zu einem solchen von der Ordnung $2m$ oder $2m+1$ führen [7]).

Von weiteren Anwendungen sei etwa erwähnt eine Kombination zwischen Gaußscher Quadratur- und Eulerscher Summenformel, wie sie kürzlich J. V. Uspensky [8]) behandelt hat. Derartige Rechnungen lassen sich leicht dem hier dargelegten Gesichtspunkt unterordnen.

---

[7]) Vgl. z. B. N. E. Nörlund, Differenzenrechnung, Berlin 1924, S. 30.

[8]) J. V. Uspensky, Bull. Amer. Mathem. Society **40** (1934), S. 871—876.

Eingegangen 1. Mai 1935.

Zur Theorie der Gleichgewichtsfiguren rotierender inhomogener Flüssigkeiten.

Von *Karl Maruhn* in Berlin.

Die vorliegende Note bringt eine Ergänzung zu den fundamentalen Existenzsätzen Lichtensteins über Gleichgewichtsfiguren rotierender inhomogener Flüssigkeiten. Ich verzichte der Kürze halber auf die Formulierung der Voraussetzungen und die umfangreiche Einführung der einzelnen Bezeichnungen und verweise auf die in Frage kommende Originalabhandlung [1]), an die ich mich in jeder Beziehung anschließe.

Bei dem Beweise der Existenz inhomogener Gleichgewichtsfiguren in der Nachbarschaft einer gegebenen Gleichgewichtsfigur mußte deren Flüssigkeit nicht durchweg von stetiger Dichte sein, vielmehr waren eine endliche Anzahl Sprungflächen zugelassen. Die Randfläche S kann ebenfalls als eine solche aufgefaßt werden, wenn die Randdichte von Null verschieden ist.

Es wird im folgenden gezeigt werden, daß im regulären Falle in der Umgebung einer Gleichgewichtsfigur, in der sich eine Sprungfläche der Dichte befindet, Gleichgewichtsfiguren durchweg stetiger Dichte liegen. Man wird dabei erkennen, daß sich auf dem gleichen Wege eine endliche Anzahl von Sprüngen ausgleichen läßt [2]). Freilich wird in der Umgebung der früheren Sprungfläche die Dichte sehr scharf zu kleineren Werten abfallen.

Anwendung findet dieses Ergebnis auf gewisse Konfigurationen, die aus einer flüssigen Kernfigur hoher Dichte und einer sie umgebenden „Atmosphäre" bestehen [3]). In deren Nachbarschaft werden also Gleichgewichtsfiguren durchweg stetiger Dichte existieren.

Jede Niveaufläche S_τ der Ausgangskonfiguration ist durch eine Zahl τ, den Abstand des Koordinatenursprunges, um den sich die Niveauflächen lagern, von dem Schnittpunkt der Fläche S_τ mit der z-Achse, charakterisiert; für S nimmt τ den Wert 1 an. Die Dichte hat auf S_τ den Wert $f(\tau)$, die Sprungfläche heiße S_{τ^*}. Es sei

$$f(\tau^* - 0) - f(\tau^* + 0) = [f], \qquad (0 < \tau^* \leqq 1). \tag{1}$$

Die Dichte $F(\tau)$ auf den Niveauflächen $S_{\tau 1}$ der gesuchten Konfiguration sei jetzt gegeben durch

$$\begin{aligned} &F(\tau) = f(\tau) && \text{für} \quad 0 \leqq \tau < \tau^*,\ \tau^* + \beta < \tau \leqq 1, \\ &F(\tau) = f(\tau^* - 0) && \text{für} \quad \tau = \tau^*, \\ &F(\tau) = f(\tau) + \varphi(\tau) && \text{für} \quad \tau^* < \tau \leqq \tau^* + \beta, \qquad \beta > 0, \text{ hinreichend klein,} \end{aligned} \tag{2}$$

[1]) Vgl. L. Lichtenstein, Untersuchungen über die Gleichgewichtsfiguren rotierender Flüssigkeiten, deren Teilchen einander nach dem Newtonschen Gesetz anziehen, Dritte Abh. Nichthomogene Flüssigkeiten. Figur der Erde, Math. Zeitschr. **36** (1933), S. 481—562. Vgl. ferner l. c. [2]), S. 91 ff.

[2]) L. Lichtenstein, Gleichgewichtsfiguren rotierender Flüssigkeiten, Berlin 1933, S. 173, wo auf das vorliegende Problem hingewiesen wird.

[3]) Vgl. l. c. [2]), S. 125 f. Ferner K. Maruhn, Über den Laplaceschen Ringkörper, Math. Zeitschr. **36** (1933), S. 122—142; Über einige Gleichgewichtsfiguren rotierender Flüssigkeiten, auf deren Oberflächen singuläre Punkte liegen, Math. Zeitschr. **38** (1934), S. 747—776, insbes. S. 764 ff.

unter $\varphi(\mathfrak{r})$ eine in $\mathfrak{r}^* < \mathfrak{r} \leqq \mathfrak{r}^* + \beta$ erklärte, dort monoton abnehmende, stetige Funktion verstanden mit

$$\varphi(\mathfrak{r}^* + 0) = [f], \qquad \varphi(\mathfrak{r}^* + \beta) = 0, \tag{3}$$

die überdies stetige, einer H-Bedingung genügende partielle Ableitungen erster Ordnung besitzt. Falls der Sprung der Randdichte ausgeglichen werden soll, muß die Fläche $S_{1+\beta}$ als Begrenzung der Ausgangsfigur aufgefaßt werden.

Um die Betrachtungen zu vereinfachen, verzichten wir hier auf die von Lichtenstein eingeführte, über ganz T erstreckte kleine Dichteänderung, setzen also $\alpha = 0$.

Es bezeichne, wie üblich, $\varkappa\mathfrak{W}_1$ das Newtonsche Potential von T_1, $\varkappa\mathfrak{W}$ dasjenige von T; ferner sei $\varkappa\mathfrak{W}_1^*$ das Potential derjenigen Massenverteilung, die man erhält, wenn man in T_1 die Dichte $F(\mathfrak{r})$ durch $f(\mathfrak{r})$ ersetzt.

Es sei jetzt

$$\varkappa\widetilde{\mathfrak{W}}_1(x_1, y_1, z_1) = \varkappa\mathfrak{W}_1(x_1, y_1, z_1) - \varkappa\mathfrak{W}_1^*(x_1, y_1, z_1) \tag{4}$$

das Newtonsche Potential des schalenförmigen Körpers $\mathfrak{T}_1^*$, der von $S_{\mathfrak{r}^*1}$ und $S_{\mathfrak{r}^*+\beta,1}$ begrenzt ist und mit Flüssigkeit der Dichte $\varphi(\mathfrak{r})$ erfüllt gedacht sei.

Aus den bekannten Gleichgewichtsbedingungen

$$\begin{aligned} &\text{für } T\text{:} \quad \varkappa\mathfrak{W}(x, y, z) + \frac{\omega^2}{2}(x^2 + y^2) = C(\mathfrak{r}), \quad C(\mathfrak{r}) \text{ auf } S_{\mathfrak{r}} \text{ konstant}, \\ &\text{für } T_1\text{:} \quad \varkappa\mathfrak{W}_1(x_1, y_1, z_1) + \frac{\omega_1^2}{2}(x_1^2 + y_1^2) = C_1(\mathfrak{r}), \quad C_1(\mathfrak{r}) \text{ auf } S_{\mathfrak{r}1} \text{ konstant}, \end{aligned} \tag{5}$$

folgt in der üblichen Weise

$$\mathfrak{W}_1(x_1, y_1, z_1) - \mathfrak{W}(x, y, z) = s(\mathfrak{r}) + \frac{\omega^2}{2\varkappa}(x^2 + y^2) - \frac{\omega_1^2}{2\varkappa}(x_1^2 + y_1^2). \tag{6}$$

Dabei ist

$$\begin{aligned} \mathfrak{W}_1(x_1, y_1, z_1) - \mathfrak{W}(x, y, z) = &[\mathfrak{W}_1(x_1, y_1, z_1) - \mathfrak{W}_1^*(x_1, y_1, z_1)] \\ &+ [\mathfrak{W}_1^*(x_1, y_1, z_1) - \mathfrak{W}(x, y, z)]. \end{aligned} \tag{7}$$

Die zweite Differenz rechter Hand läßt, wie l. c. [1]) gezeigt wird, die Entwicklung

$$\begin{aligned} &\mathfrak{W}_1^*(x_1, y_1, z_1) - \mathfrak{W}(x, y, z) \\ &= \int_{T_1} f(\mathfrak{r}') \frac{d\tau_1'}{\varrho_1} - \int_T f(\mathfrak{r}') \frac{d\tau'}{\varrho} = \zeta \frac{\partial\mathfrak{W}}{\partial\nu} - \int_0^\infty df(\mathfrak{r}') \int_{S_{\mathfrak{r}'}} \zeta' \frac{d\sigma'}{\varrho} + \mathfrak{W}^{(2)} + \mathfrak{W}^{(3)} + \cdots [4]) \end{aligned} \tag{8}$$

zu, unter den $\mathfrak{W}^{(n)}$ Integralausdrücke n-ten Grades der Variablen ζ und ihrer partiellen Ableitungen erster Ordnung verstanden. Mit Rücksicht auf (8) und (4) nimmt die Integro-Differentialgleichung unseres Problems daher die Gestalt

$$\begin{aligned} \psi\zeta - \int_0^\infty df(\mathfrak{r}') \int_{S_{\mathfrak{r}'}} \zeta' \frac{d\sigma'}{\varrho} &= s(\mathfrak{r}) - \lambda(x^2 + y^2) - \widetilde{\mathfrak{W}}_1(x_1, y_1, z_1) \\ &- \frac{\omega_1^2}{2\varkappa}\zeta^2(a^2 + b^2) - 2\lambda\zeta(ax + by) - \frac{1}{\varkappa}(\mathfrak{W}^{(2)} + \mathfrak{W}^{(3)} + \cdots), \end{aligned} \tag{9}$$

an, wo $\psi = \psi(x, y, z)$ die Gesamtschwerkraft in (x, y, z) bedeutet. Die Forderung, daß der Koordinatenursprung O bei der durch ζ vermittelten Abbildung in sich selbst übergeht,

---

[4]) In unserem Falle ist zwar die eine der beiden aufeinander bezogenen Figuren keine Gleichgewichtsfigur, doch wird das Bestehen der Gleichgewichtsbedingungen bei Aufstellung der Entwicklung (8) auch gar nicht benutzt. — Die Funktion $\zeta = \zeta(x, y, z)$ bezeichnet den Abstand des Punktes (x_1, y_1, z_1) der gesuchten Konfiguration von dem korrespondierenden Punkte (x, y, z) der gegebenen Verteilung. Die beiden Punkte liegen auf der gleichen, durch (x, y, z) verlaufenden Normalen zu der durch diesen Punkt gehenden Ausgangsniveaufläche.

liefert dann noch die Gleichung (9) in der Form

$$(10)\quad \psi\zeta - \int_0^\infty df(\mathfrak{r}') \int_{S_{\mathfrak{r}'}} \zeta' \left(\frac{1}{\varrho} - \frac{1}{{}_0\varrho}\right) d\sigma'_{\mathfrak{r}} = h\mathfrak{r}^2\mathfrak{F}(\mathfrak{r}) - \lambda(x^2+y^2)$$
$$- [\mathfrak{W}_1(x_1, y_1, z_1) - \mathfrak{W}_1(0,0,0)] - \frac{\omega_1^2}{2\varkappa}\zeta^2(a^2+b^2) - 2\lambda\zeta(ax+by)$$
$$- \frac{1}{\varkappa}(\mathfrak{W}^{(2)} + \mathfrak{W}^{(3)} + \cdots - {}_0\mathfrak{W}^{(2)} - {}_0\mathfrak{W}^{(3)} - \cdots).$$

Die Gleichungen (9) und (10) sind den l. c. [1]) angegebenen Gleichungen gegenüber lediglich um das Glied $\mathfrak{W}_1(x_1, y_1, z_1)$ bzw. $\mathfrak{W}_1(x_1, y_1, z_1) - \mathfrak{W}_1(0,0,0)$ vermehrt, das wir nunmehr einigen Abschätzungen unterwerfen wollen.

Nach Voraussetzung sind die Niveauflächen $S_{\mathfrak{r}1}$ des Gesamtpotentials U_1 der gesuchten Konfiguration alle ineinandergeschachtelt und besitzen eine stetige Normale. Man erkennt leicht, daß

$$(11)\qquad \mathfrak{W}_1(x_1, y_1, z_1) = \int_{\mathfrak{T}_1^*} \varphi(\mathfrak{r}') \frac{1}{\varrho_1} d\sigma'_{\mathfrak{r}1} dv'_{\mathfrak{r}1}$$

gilt, unter $d\sigma'_{\mathfrak{r}1}$ das Flächenelement auf $S_{\mathfrak{r}1}$, unter $\nu_{\mathfrak{r}1}$ die nach außen gerichteten Normalen zu $S_{\mathfrak{r}1}$ verstanden. Beachten wir, daß die Gesamtschwerkraft ψ_1 der gesuchten Konfiguration stets der Richtung $\nu_{\mathfrak{r}1}$ entgegengesetzt wirkt, so erhalten wir

$$(12)\qquad dU_1 = -\psi_1 d\nu_{\mathfrak{r}1}\,.$$

Wir schreiben daher $\mathfrak{W}_1$ mit Rücksicht auf (11) jetzt in der Gestalt

$$(13)\qquad \mathfrak{W}_1(x_1, y_1, z_1) = \int_{U_1(\mathfrak{r}_1^*+\beta_1)}^{U_1(\mathfrak{r}_1^*)} \varphi_1(\mathfrak{r}'_1)\, dU'_1 \int_{S_{\mathfrak{r}'1}} \frac{1}{\psi'_1}\frac{d\sigma'_{\mathfrak{r}1}}{\varrho_1}, \qquad \varphi_1(\mathfrak{r}_1) = \varphi(\mathfrak{r}).$$

Dabei charakterisiert $\mathfrak{r}_1$ (genau wie $\mathfrak{r}$ bei der Ausgangskonfiguration) die Fläche $S_{\mathfrak{r}1}$ und bedeutet geometrisch den Abstand des Koordinatenursprungs von dem Schnittpunkt der z_1-Achse (die mit der z-Achse koinzidiert) mit $S_{\mathfrak{r}1}$. Aus Gründen der vorausgesetzten Symmetrie steht die z_1-Achse auf allen Flächen $S_{\mathfrak{r}1}$ senkrecht. Das in (13) auftretende Integral ist ein Integral im Sinne von Stieltjes.

Zunächst einige Worte über die Größe β_1. Es ist

$$(14)\quad \beta_1 = (\mathfrak{r}_1^* + \beta_1) - \mathfrak{r}_1^* = [\mathfrak{r}^* + \beta + \zeta(0,0,\mathfrak{r}^*+\beta)] - [\mathfrak{r}^* + \zeta(0,0,\mathfrak{r}^*)]$$
$$= \beta + \zeta(0,0,\mathfrak{r}^*+\beta) - \zeta(0,0,\mathfrak{r}^*)\,.$$

Nach Voraussetzung ist ζ in $T+S$ stetig und besitzt stetige, allenfalls abteilungsweise stetige partielle Ableitungen erster Ordnung. Ist nun, unter Ω eine hinreichend kleine positive Zahl verstanden,

$$(15)\qquad \left|\frac{\partial\zeta}{\partial x}\right|, \left|\frac{\partial\zeta}{\partial y}\right|, \left|\frac{\partial\zeta}{\partial z}\right| \leqq \Omega,\ |\zeta| \leqq \sqrt{3}\,\Omega r, \qquad (r^2 = x^2+y^2+z^2),$$

so finden wir

$$(16)\qquad \beta_1 \leqq c_1\beta(1+\Omega)\,,$$

wo c_1 eine positive Konstante ist, wie auch später $c_2, \ldots$

Wir wenden uns nunmehr den Ableitungen $\frac{\partial\mathfrak{W}_1}{\partial x_1}, \frac{\partial\mathfrak{W}_1}{\partial y_1}, \frac{\partial\mathfrak{W}_1}{\partial z_1}$ zu und nehmen zunächst an, daß der Punkt (x_1, y_1, z_1) in $\mathfrak{T}_1^* + S_{\mathfrak{r}^*1} + S_{\mathfrak{r}^*+\beta,1}$ gelegen sei. Aus $\mathfrak{T}_1^*$ schneiden wir alsdann einen Bereich Θ_1 aus (vgl. Fig. 1) durch denjenigen Kreiszylinder vom

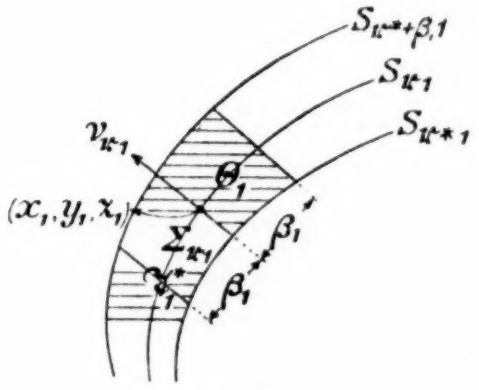

Fig. 1.

Querschnittradius β_1, der die zu (x_1, y_1, z_1) gehörige Normale $\nu_{\mathfrak{r}1}$ zur Achse hat [5]). Die hierbei aus den Flächen $S_{\mathfrak{r}1}$ ausgeschnittenen Flächenstücke mögen $\Sigma_{\mathfrak{r}1}$ heißen. Alsdann ist etwa

$$(17)\quad \frac{\partial \widetilde{\mathfrak{W}}_1}{\partial x_1} = \frac{\partial}{\partial x_1}\int_{\Theta_1} \varphi(\mathfrak{r}')\,\frac{d\tau_1'}{\varrho_1} + \int_{U_1(\mathfrak{r}_1^*+\beta_1)}^{U_1(\mathfrak{r}_1^*)} \varphi_1(\mathfrak{r}_1')\,dU_1' \frac{\partial}{\partial x_1}\int_{S_{\mathfrak{r}'1}-\Sigma_{\mathfrak{r}'1}} \frac{1}{\psi_1'}\,\frac{d\sigma_{\mathfrak{r}1}'}{\varrho_1} = \Phi_1 + \Phi_2\,.$$

Wir bezeichnen weiter mit $\mathfrak{V}_1$ das Volumen des von dem Kreiszylinder ausgeschnittenen Bereiches Θ_1. Wegen

$$(18)\qquad \mathfrak{V}_1 = \int_{U_1(\mathfrak{r}_1^*+\beta_1)}^{U_1(\mathfrak{r}_1^*)} dU_1' \int_{\Sigma_{\mathfrak{r}'1}} \frac{d\sigma_{\mathfrak{r}1}'}{\psi_1}$$

erkennt man leicht, daß sich für hinreichend kleine Werte von β und daher, mit Rücksicht auf (14), auch von β_1 eine Konstante c_2 derart finden läßt, daß gleichmäßig für alle in $\mathfrak{T}_1^* + S_{\mathfrak{r}^*1} + S_{\mathfrak{r}^*+\beta,1}$ gelegenen Punkte (x_1, y_1, z_1)

$$(19)\qquad \mathfrak{V}_1 \leqq c_2\beta_1^3$$

gilt. Nach einem Hilfssatz von Herrn E. Schmidt [6]) ist nunmehr

$$(20)\qquad |\Phi_1| < [f]\int_{\Theta_1} \frac{d\tau_1'}{\varrho_1^2} \leqq 4\pi\,[f]\left(\frac{3\mathfrak{V}_1}{4\pi}\right)^{1/3} \leqq c_3\beta_1 \leqq c_4\beta(1+\Omega)\,.$$

Ferner folgt aus bekannten Sätzen über die Ableitungen von Potentialen einfacher Flächenbelegungen für hinreichend kleine Werte von β

$$(21)\quad |\Phi_2| \leqq c_5\beta_1|\log\beta_1| \leqq c_6\beta(1+\Omega)\,(|\log\beta| + \log(1+\Omega)) \leqq c_7(1+\Omega)\beta\,|\log\beta|\,.$$

Alles in allem ist somit

$$(22)\qquad \left|\frac{\partial\widetilde{\mathfrak{W}}_1}{\partial x_1}\right|,\ \left|\frac{\partial\widetilde{\mathfrak{W}}_1}{\partial y_1}\right|,\ \left|\frac{\partial\widetilde{\mathfrak{W}}_1}{\partial z_1}\right| \leqq c_8(1+\Omega)\beta\,|\log\beta|$$

und wegen $x_1 = x + a\zeta$, $y_1 = y + b\zeta$, $z_1 = z + c\zeta$ (a, b, c die Richtungskosinus der Normalen zu $S_{\mathfrak{r}}$) auch

$$(23)\qquad \left|\frac{\partial\widetilde{\mathfrak{W}}_1}{\partial x}\right|,\ \left|\frac{\partial\widetilde{\mathfrak{W}}_1}{\partial y}\right|,\ \left|\frac{\partial\widetilde{\mathfrak{W}}_1}{\partial z}\right| \leqq c_9(1+\Omega)\,\beta\,|\log\beta|\,.$$

Mit

$$(24)\qquad \beta\,|\log\beta| = \Omega^*$$

---

[5]) Vgl. die nachgelassene Arbeit von L. Lichtenstein, Zur Theorie der Gleichgewichtsfiguren homogener Flüssigkeiten, Math. Zeitschr. **39** (1935), S. 639—648, wo sich ähnliche Betrachtungen finden.

[6]) E. Schmidt, Bemerkungen zur Potentialtheorie, Schwarz-Festschrift, Berlin 1914, S. 365—383, insbes. S. 368.

und mit Rücksicht auf die vorausgesetzten Symmetrieeigenschaften ist dann

$$\left|\frac{\partial}{\partial x}\widetilde{\mathfrak{W}}_1\right|,\ \left|\frac{\partial}{\partial y}\widetilde{\mathfrak{W}}_1\right|,\ \left|\frac{\partial}{\partial z}\widetilde{\mathfrak{W}}_1\right| \leqq c_{10}\,\Omega^*(1+\Omega)r\,,$$

$$|\,\widetilde{\mathfrak{W}}_1(x_1, y_1, z_1) - \widetilde{\mathfrak{W}}_1(0,0,0)| \leqq c_{10}\sqrt{3}\,\Omega^*(1+\Omega)\,r^2\,. \tag{25}$$

Liegt der Aufpunkt außerhalb des genannten Bereiches, so läßt sich gewiß die Konstante c_9 so wählen, daß (23) gleichmäßig für alle (x_1, y_1, z_1) gilt.

Es bezeichne weiter ζ eine ganz wie ζ beschaffene Funktion mit

$$\left|\frac{\partial\zeta}{\partial x}-\frac{\partial\dot\zeta}{\partial x}\right|,\ \left|\frac{\partial\zeta}{\partial y}-\frac{\partial\dot\zeta}{\partial y}\right|,\ \left|\frac{\partial\zeta}{\partial z}-\frac{\partial\dot\zeta}{\partial z}\right| \leqq \Xi \leqq 2\Omega, \qquad |\zeta-\dot\zeta| \leqq \sqrt{3}\,\Xi r\,. \tag{26}$$

$\dot{\widetilde{\mathfrak{W}}}_1$ sei das $\widetilde{\mathfrak{W}}_1$ entsprechende Raumpotential. Dann ist [7]), wieder mit Rücksicht auf die Symmetrieeigenschaften,

$$\left|\frac{\partial}{\partial x}(\widetilde{\mathfrak{W}}_1-\dot{\widetilde{\mathfrak{W}}}_1)\right|,\ \left|\frac{\partial}{\partial y}(\widetilde{\mathfrak{W}}_1-\dot{\widetilde{\mathfrak{W}}}_1)\right|,\ \left|\frac{\partial}{\partial z}(\widetilde{\mathfrak{W}}_1-\dot{\widetilde{\mathfrak{W}}}_1)\right| \leqq c_{11}\,\Xi r\,,$$

$$|(\widetilde{\mathfrak{W}}_1(x_1,y_1,z_1)-\widetilde{\mathfrak{W}}_1(0,0,0))-(\dot{\widetilde{\mathfrak{W}}}_1(\dot x_1,\dot y_1,\dot z_1)-\dot{\widetilde{\mathfrak{W}}}_1(0,0,0))| \leqq c_{11}\sqrt{3}\,\Xi r\,. \tag{27}$$

Andererseits folgt aus (25)

$$\left|\frac{\partial}{\partial x}(\widetilde{\mathfrak{W}}_1-\dot{\widetilde{\mathfrak{W}}}_1)\right|,\ \left|\frac{\partial}{\partial y}(\widetilde{\mathfrak{W}}_1-\dot{\widetilde{\mathfrak{W}}}_1)\right|,\ \left|\frac{\partial}{\partial z}(\widetilde{\mathfrak{W}}_1-\dot{\widetilde{\mathfrak{W}}}_1)\right| \leqq c_{12}\,\Omega^* r\,,$$

$$|(\widetilde{\mathfrak{W}}_1(x_1,y_1,z_1)-\widetilde{\mathfrak{W}}_1(0,0,0))-(\dot{\widetilde{\mathfrak{W}}}_1(\dot x_1,\dot y_1,\dot z_1)-\dot{\widetilde{\mathfrak{W}}}_1(0,0,0))| \leqq c_{12}\sqrt{3}\,\Omega^* r^2\,. \tag{28}$$

In den Beziehungen (27) und (28) dürfen dabei den Größen Ξ und Ω^* unabhängig voneinander alle Werte der Intervalle $0 \leqq \Xi \leqq 2\Omega$, $0 \leqq \Omega^* \leqq \varepsilon$ ($\varepsilon > 0$, hinreichend klein) zuerteilt werden. Halten wir etwa in (28) für den Moment Ω^* fest, so muß, damit (27) erfüllt ist,

$$c_{12} \leqq c_{13}\Xi \tag{29}$$

gelten. Wir haben daher schließlich

$$\left|\frac{\partial}{\partial x}(\widetilde{\mathfrak{W}}_1-\dot{\widetilde{\mathfrak{W}}}_1)\right|,\ \left|\frac{\partial}{\partial y}(\widetilde{\mathfrak{W}}_1-\dot{\widetilde{\mathfrak{W}}}_1)\right|,\ \left|\frac{\partial}{\partial z}(\widetilde{\mathfrak{W}}_1-\dot{\widetilde{\mathfrak{W}}}_1)\right| \leqq c_{14}\,\Omega^*\,\Xi r\,,$$

$$|(\widetilde{\mathfrak{W}}_1(x_1,y_1,z_1)-\widetilde{\mathfrak{W}}_1(0,0,0))-(\dot{\widetilde{\mathfrak{W}}}_1(\dot x_1,\dot y_1,\dot z_1)-\dot{\widetilde{\mathfrak{W}}}_1(0,0,0))| \leqq c_{14}\sqrt{3}\,\Omega^*\,\Xi r^2\,. \tag{30}$$

Nach Feststellung der Beziehungen (25) und (30) bietet auf Grund der schon über die rechten Seiten von (9) und (10) bekannten Abschätzungen die weitere Behandlung keine neuen Schwierigkeiten dar.

---

[7]) Vgl. L. Lichtenstein, Über einige Hilfssätze der Potentialtheorie IV, Sächs. Berichte **82** (1930), S. 265—344, ferner auch l. c. [1]).

Eingegangen 22. Mai 1935.

Operatoren im Wachsschen Raum [1]).

Von *Oswald Teichmüller* in Göttingen.

Inhaltsverzeichnis.

		Seite
§ 1.	Der Grundkörper	74
§ 2.	Der Raum	74
§ 3.	Operatoren	79
§ 4.	Vertauschbarkeit	82
§ 5.	Die Dimension	85
§ 6.	Weitere Sätze über die Dimension	88
§ 7.	Der Spektralsatz	93
§ 8.	Quaternionendarstellungen	95
§ 9.	Normalformen für Imaginäroperatoren	99
§ 10.	Hermitesche abgeschlossene Operatoren	104
§ 11.	Nurmaximale Operatoren im Wachsschen Raum	107
§ 12.	Propädeutische Betrachtung normaler Operatoren	111
§ 13.	Beschränkte normale Operatoren	116
§ 14.	Beweis des Hauptsatzes	120

Einleitung.

H. Wachs sprach 1934 den Gedanken aus, einen zum Hilbertschen Raum analogen Raum mit Koeffizienten aus dem Quaternionenkörper aufzubauen. Das wird in dieser Arbeit geschehen. Es ergibt sich dabei zunächst, bei zweckmäßigen Grunddefinitionen, eine weitgehende Analogie zum Hilbertschen Raum und seiner Operatorentheorie, so daß sich die meisten Definitionen und Sätze wörtlich übertragen. An zwei Stellen jedoch, bei der Fortsetzungstheorie abgeschlossener hermitescher Operatoren nämlich und beim Spektralproblem der normalen Operatoren, waren neue Überlegungen nötig, die auch zu anderen Ergebnissen führten, als den aus dem Hilbertschen Raum bekannten. Die neuen Sätze und Beweise ließen sich in den Hilbertschen Raum und den reellen Hilbertschen Raum übertragen und ergaben neue Gesichtspunkte und Einordnungen für die dort bekannten Tatsachen. Selbstverständlich werden alle unwesentlichen Dimensionsbeschränkungen fortgelassen. Auf physikalische Anwendungen gehe ich nicht ein, möchte es aber nicht unterlassen, auf eine Arbeit von Jordan [1] hinzuweisen [2]), wo von einer möglichen Anwendung von Quaternionenmatrizen in der relativistischen Quantenmechanik die Rede ist.

In §§ 1—3 werden die Bezeichnungen eingeführt und die wichtigsten Sätze der bekannten Theorie ohne ausführliche Beweise übertragen. In § 4, der ebenfalls einleitenden Charakter hat, werden die Sätze über vertauschbare Operatoren zusammengestellt, insbesondere wird der Reduktionsbegriff gleich so eingeführt, wie er später

[1]) Diese Arbeit wurde von der Mathematisch-Naturwissenschaftlichen Fakultät der Ernst-August-Universität zu Göttingen als Dissertation angenommen. Referent war Herr Prof. Dr. Hasse.

[2]) Die in eckigen Klammern beigefügten Nummern verweisen auf das Literaturverzeichnis am Ende der Arbeit.

gebraucht wird. Die §§ 5 und 6 bringen dann, vom eigentlichen Thema abschweifend, eine ausführliche Theorie der Dimension. Der lokale Zerlegungssatz, den Rieß [1] als eigentlichen Kern des Spektralsatzes über selbstadjungierte Operatoren erkannte, wird in § 7 mit Hilfe eines Formalismus, der auf eine Arbeit von v. Neumann [3] zurückgeht, bewiesen; derselbe Formalismus wird auch später in § 14 angewandt. Dann folgt, nach Vorbereitungen in §§ 8 und 9, in § 10 die allgemeine Fortsetzungstheorie der hermiteschen abgeschlossenen Operatoren, die die v. Neumannsche Theorie als Spezialfall enthält. Eine rechnerische Bestimmung aller maximalen, aber nicht selbstadjungierten Operatoren im Wachsschen Raum (§ 11) schließt sich an. Schließlich versuche ich in den §§ 12—14 das Spektralproblem der normalen Operatoren zu lösen. Als elementare Bausteine ergeben sich dabei allerdings neben den Projektoren, mit denen man im Hilbertschen Raum auskommt, notwendigerweise noch die in § 9 näher untersuchten „Imaginäroperatoren".

§ 1. Der Grundkörper.

Σ sei entweder der Körper R der reellen Zahlen oder der Körper K der komplexen Zahlen oder der Quaternionenkörper Q. Z sei das Zentrum von Σ, also R bzw. K bzw. R. Wir benutzen folgende Basis von Σ über R:

$$\begin{aligned} R &= 1R, \\ K &= 1R + iR && (i^2 = -1), \\ Q &= 1R + iR + jR + kR && (i^2 = j^2 = -1,\ ij = k = -ji). \end{aligned}$$

Wir wollen uns K immer als den speziellen Unterkörper $R(i)$ von Q vorstellen.

Ein (durch algebraische Eigenschaften ausgezeichneter) inverser Automorphismus $a \to \bar{a}$ von Σ über dem Fixkörper R wird gegeben durch

$$\begin{aligned} \bar{a} &= a \quad \text{für} \quad a \in R, \\ \bar{i} &= -i, \quad \bar{j} = -j, \quad \bar{k} = -k. \end{aligned}$$

Er hat die Haupteigenschaften:

$$\begin{aligned} \bar{a} + \bar{b} &= \overline{a+b}, \\ \bar{a}\bar{b} &= \overline{ba}, \\ \bar{\bar{a}} &= a, \\ a + \bar{a} &\in R, \\ \bar{a}a = a\bar{a} &\geqq 0 \text{ in } R,\ \bar{a}a = 0 \text{ nur wenn } a = 0. \end{aligned}$$

Und definiert man

$$|a| = \sqrt{\bar{a}a} \geqq 0,$$

so gilt

$$\begin{aligned} |ab| &= |a|\,|b|, \\ |a+b| &\leqq |a| + |b|. \end{aligned}$$

Zu jedem $a \in Q$ gibt es ein $c \neq 0$ in Q so, daß

$$b = c^{-1}ac \in K,\ \frac{b-\bar{b}}{2i} \geqq 0.$$

All diese Bezeichnungen und Regeln werden in der ganzen Arbeit stillschweigend angewandt.

§ 2. Der Raum.

1. Unter einem *Raum* verstehen wir in dieser Arbeit eine nichtleere Menge $\mathfrak{R}$, die (im Sinne der abstrakten Algebra) in dreifacher Weise mit dem „Grundkörper" Σ

verknüpft ist:

1) Zu $x \in \mathfrak{R}$, $y \in \mathfrak{R}$ gibt es ein $x + y \in \mathfrak{R}$.
2) Zu $x \in \mathfrak{R}$, $a \in \Sigma$ gibt es ein $xa \in \mathfrak{R}$.
3) Zu $x \in \mathfrak{R}$, $y \in \mathfrak{R}$ gibt es ein $(x, y) \in \Sigma$.

Und zwar sollen diese drei „Verknüpfungen" folgenden sechs Axiomen genügen, in denen a ein Element von Σ und x, y, z, x_n Elemente aus $\mathfrak{R}$ bezeichnen:

1) $(x + y, z) = (x, z) + (y, z)$.
2) $(xa, y) = (x, y)a$.
3) Gilt $(x, z) = (y, z)$ für alle z, so ist $x = y$.
4) $(y, x) = \overline{(x, y)}$.
5) $(x, x) \geqq 0$.
6) Gilt $\lim\limits_{m,n\to\infty} (x_m + x_n(-1), x_m + x_n(-1)) = 0$, so gibt es ein $x \in \mathfrak{R}$ mit
$$\lim_{n\to\infty} (x + x_n(-1), x + x_n(-1)) = 0.$$

2. Um zu erkennen, inwiefern der so erklärte Raum eine vernünftige Verallgemeinerung des Hilbertschen Raums ist, ziehen wir sofort die einfachsten Folgerungen aus den Axiomen.

Weil identisch für alle z
$$(x + y, z) = (x, z) + (y, z) = (y, z) + (x, z) = (y + x, z)$$
gilt, ist nach Axiom 3)
$$x + y = y + x.$$
Genau so beweist man unter alleiniger Benutzung der Axiome 1)—3):
$$(x + y) + z = x + (y + z).$$
$$(x + y(-1)) + y = x.$$
$$(x + y)a = xa + ya.$$
$$x(a + b) = xa + xb.$$
$$x(ab) = (xa)b.$$
$$x1 = x.$$
Das drückt man bekanntlich so aus: $\mathfrak{R}$ ist (hinsichtlich der ersten beiden Raumverknüpfungen) ein Σ-Rechtsmodul. Wie immer erklärt man
$$x + y(-1) = x - y, \quad x - x = 0, \quad 0 - x = -x;$$
dann ist
$$0a = x0 = 0, \quad -x = x(-1) \text{ usw.}$$

Aus 2) und 4) folgt
$$(x, yb) = \overline{(yb, x)} = \overline{(y, x)b} = \bar{b}\,\overline{(y, x)} = \bar{b}(x, y),$$
also
$$(xa, yb) = \bar{b}(x, y)a.$$
Setzt man
$$|x| = \sqrt{(x, x)} \geqq 0,$$
so ist
$$|xa| = |a|\,|x|,$$
und aus
$$0 \leqq |x\lambda + y(x, y)\mu|^2 = \lambda |x|^2 \lambda + \mu\,\overline{(x, y)}\,(x, y)\,\lambda + \lambda\,(y, x)\,(x, y)\,\mu + \mu\,\overline{(x, y)}\,|y|^2\,(x, y)\mu$$
für alle reellen λ und μ folgt für die Diskriminante
$$|x|^2\,|y|^2\,|(x, y)|^2 - |(x, y)|^4 \geqq 0,$$
$$|(x, y)| \leqq |x|\,|y|.$$

Aus dieser Schwarzschen Ungleichung folgt wie üblich die Dreiecksungleichung

$$|x + y| \leqq |x| + |y|.$$

Aus $|x| = 0$ folgt $x = 0$. Für alle z ist nämlich

$$0 \leqq |(x, z)| \leqq |x|\,|z| = 0,$$

$$(x, z) = (0, z),$$

sowie $|x| = 0$; nach 3) folgt $x = 0$.

Jetzt sieht man, daß unsere Axiome bis auf größere Allgemeinheit des Grundkörpers und der Dimension mit den bekannten Axiomen des Hilbertschen Raums übereinstimmen [3]).

Wir können es uns darum ersparen, alle Einzelheiten des weiteren Aufbaus, soweit es sich um bloße Verallgemeinerungen bekannter Schlüsse handelt, ausführlich durchzurechnen; es wird vielmehr genügen, unter Verweis auf die Literatur des Hilbertschen Raums die Hauptergebnisse anzugeben. Man hat dabei eigentlich nur im Auge zu behalten, daß die Faktoren aus Σ immer rechts von den Elementen aus $\mathfrak{R}$ stehen, und die Regel

$$(xa, yb) = \bar{b}(x, y)\,a$$

zu beachten.

Gibt es zu der Folge x_n aus $\mathfrak{R}$ ein $x \in \mathfrak{R}$ mit $\lim_{n\to\infty} |x - x_n| = 0$, so gibt es nur eins; dies heißt dann $x = \lim_{n\to\infty} x_n$. Das innere Produkt ist stetig, d. h. aus $\lim_{n\to\infty} x_n = x$, $\lim_{n\to\infty} y_n = y$ folgt

$$\lim_{n\to\infty} (x_n, y_n) = (x, y).$$

Für $(x, y) = 0$ schreibt man auch: $x \perp y$. Für Mengen $\mathfrak{M}, \mathfrak{N} \leqq \mathfrak{R}$ bedeute $\mathfrak{M} \perp \mathfrak{N}$, daß $x \perp y$ für alle $x \in \mathfrak{M}$, $y \in \mathfrak{N}$.

3. Ein *Orthonormalsystem* (normiertes Orthogonalsystem) ist eine Teilmenge $\mathfrak{P}$ von $\mathfrak{R}$ mit der Eigenschaft, daß für $p \in \mathfrak{P}$, $q \in \mathfrak{P}$ stets gilt

$$(p, q) = \begin{cases} 1, & p = q \\ 0, & p \neq q. \end{cases}$$

Die Haupteigenschaft der Orthonormalsysteme ist die Besselsche Ungleichung: für jedes $x \in \mathfrak{R}$ gilt, wenn $p_1, p_2, \ldots, p_m$ verschiedene Elemente von $\mathfrak{P}$ sind,

$$|x|^2 - |(x, p_1)|^2 - \cdots - |(x, p_m)|^2 \geqq 0.$$

Aus ihr folgt: $\sum_{p\in\mathfrak{P}} p(x, p)$ ist für jedes x in dem Sinne konvergent, daß alle Glieder bis auf höchstens abzählbar viele verschwinden und bei beliebiger Numerierung der übrigen Glieder der Limes der Partialsummen existiert. Ist

$$x = \sum_{\mathfrak{P}} p(x, p) \quad \text{für alle } x \in \mathfrak{R},$$

so heißt $\mathfrak{P}$ *vollständig*.

Es gibt ein vollständiges Orthonormalsystem in $\mathfrak{R}$.

Beweis: Sei eine Wohlordnung von $\mathfrak{R}$ gegeben. Dann werde $\mathfrak{P}$ durch transfinite Induktion [4]) erklärt: p werde dann und nur dann in $\mathfrak{P}$ aufgenommen, wenn $|p| = 1$ und $p \perp q$ ist für alle diejenigen Vorgänger q von p (in der Wohlordnung), die schon

---

[3]) v. Neumann [1] I § 2.

[4]) Daß man Funktionen durch transfinite Induktion erklären kann, ist bekannt (v. d. Waerden [1] § 59). Teilmengen $\mathfrak{P}$ von $\mathfrak{R}$ kann man aber durch ihre charakteristische Funktion ($\chi(x) = 1$ für $x \in \mathfrak{P}$, $= 0$ sonst) beschreiben.

in $\mathfrak{P}$ aufgenommen sind. Daß das so konstruierte $\mathfrak{P}$ ein Orthonormalsystem ist, ist klar. Wäre $\mathfrak{P}$ nicht vollständig, so gäbe es ein $x \in \mathfrak{R}$ mit

$$y = x - \sum_{\mathfrak{P}} p(x, p) \neq 0 .$$

Setzt man

$$z = y|y|^{-1},$$

so wäre, wie man leicht nachrechnet, $|z| = 1$ und $z \perp q$ für alle $q \in \mathfrak{P}$, insbesondere $z \perp q$ für alle Vorgänger q von z, die in $\mathfrak{P}$ enthalten sind; nach Konstruktionsvorschrift von $\mathfrak{P}$ müßte z in $\mathfrak{P}$ aufgenommen worden sein, daher $z \perp z$, was sich mit $|z| = 1$ nicht verträgt.

Schon oben benutzten wir: Wird jedem $p \in \mathfrak{P}$ ein $\xi_p \in \Sigma$ so zugeordnet, daß (höchstens abzählbar viele $\xi_p \neq 0$ sind und) $\sum_{\mathfrak{P}} |\xi_p|^2$ konvergiert, so konvergiert $\sum_{\mathfrak{P}} p\,\xi_p$. Damit haben wir eine vollständige Übersicht über alle Räume: Es gibt ein vollständiges Orthonormalsystem $\mathfrak{P}$, und die Elemente von $\mathfrak{R}$ sind genau die Summen

$$\sum_{\mathfrak{P}} p\,\xi_p ,$$

wo die ξ_p Elemente von Σ mit (im erklärten Sinne) konvergenter $\sum_{\mathfrak{P}} |\xi_p|^2$ sind. Und ist $x = \sum_{\mathfrak{P}} p\,\xi_p$, $y = \sum_{\mathfrak{P}} p\,\eta_p$, so drücken sich die drei Raumverknüpfungen (Addition, hintere skalare Multiplikation, inneres Produkt) folgendermaßen durch die „Koordinaten" ξ_p, η_p aus:

$$x + y = \sum_{\mathfrak{P}} p(\xi_p + \eta_p) ,$$

$$xa = \sum_{\mathfrak{P}} p(\xi_p a),$$

$$(x, y) = \sum_{\mathfrak{P}} \overline{\eta}_p \xi_p \quad \text{(sic!)}.$$

Von diesen Formeln ausgehend, kann man ähnlich wie Löwig[5]) Beispiele von Räumen konstruieren, wobei man noch den Grundkörper Σ und die Mächtigkeit des vollständigen Orthonormalsystems, von dem man ausgeht, beliebig vorgeben kann.

4. Nachdem wir so einen Überblick über die Beziehungen zwischen den Elementen des Raumes $\mathfrak{R}$ gewonnen haben, wenden wir uns zur Betrachtung von Teilmengen von $\mathfrak{R}$.

Unter einer Linearmannigfaltigkeit versteht man eine nichtleere Teilmenge von $\mathfrak{R}$, die mit x und y stets auch alle $xa + yb$ (a und b beliebig aus Σ) enthält. Ist $\mathfrak{M}$ eine Teilmenge von $\mathfrak{R}$, so ist die Menge aller endlichen Summen Σxa mit $x \in \mathfrak{M}$, $a \in \Sigma$ (bzw. 0, wenn $\mathfrak{M}$ leer ist) die kleinste $\mathfrak{M}$ enthaltende Linearmannigfaltigkeit und heißt *die von $\mathfrak{M}$ erzeugte Linearmannigfaltigkeit*; sie werde mit $\widehat{\mathfrak{M}}$ bezeichnet. Für die nur aus 0 bestehende Linearmannigfaltigkeit werden wir ohne Verwechslungsgefahr 0 schreiben. Ist eine Linearmannigfaltigkeit $\mathfrak{M}$ abgeschlossen, d. h. enthält $\mathfrak{M}$ mit jeder konvergenten Folge auch ihr Grenzelement, so lassen sich in $\mathfrak{M}$ nicht nur alle Raumverknüpfungen ausführen, sondern es gelten auch alle sechs Axiome (insbesondere 6)); $\mathfrak{M}$ kann daher *Unterraum* genannt werden. Ist $\mathfrak{M}$ wieder eine beliebige Teilmenge von $\mathfrak{R}$, so ist die Menge der Grenzen aller konvergenten Folgen aus $\widehat{\mathfrak{M}}$ (die abgeschlossene Hülle von $\widehat{\mathfrak{M}}$) der kleinste $\mathfrak{M}$ enthaltende Unterraum und heißt *der von $\mathfrak{M}$ erzeugte Unterraum*, geschrieben $\widetilde{\mathfrak{M}}$. Eine Menge $\mathfrak{M}$ heißt in der Menge $\mathfrak{N}$ *dicht*, wenn jedes Element von $\mathfrak{N}$ Grenze einer Folge aus $\mathfrak{M}$ ist.

Der Durchschnitt von $\mathfrak{M}$ und $\mathfrak{N}$ werde mit $\mathfrak{M} \cap \mathfrak{N}$ bezeichnet. Sind $\mathfrak{M}$ und $\mathfrak{N}$ Linearmannigfaltigkeiten, die nur 0 gemein haben, so bezeichnen wir die von $\mathfrak{M}$ und $\mathfrak{N}$ erzeugte Linearmannigfaltigkeit mit $\mathfrak{M} \dot{+} \mathfrak{N}$; sind $\mathfrak{M}$ und $\mathfrak{N}$ sogar Unterräume und ist

[5]) Löwig [1] S. 25f.

$\mathfrak{M} \perp \mathfrak{N}$, so bezeichnen wir die von $\mathfrak{M}$ und $\mathfrak{N}$ erzeugte Linearmannigfaltigkeit, die dann sogar ein Unterraum ist, mit $\mathfrak{M} \oplus \mathfrak{N}$ [6]). Sind $\mathfrak{M}$ und $\mathfrak{N}$ Unterräume, $\mathfrak{M} \supseteqq \mathfrak{N}$, so sei $\mathfrak{M} \ominus \mathfrak{N}$ die Menge der $x \in \mathfrak{M}$ mit $x \perp \mathfrak{N}$. Dies $\mathfrak{M} \ominus \mathfrak{N}$ heißt das orthogonale Komplement von $\mathfrak{N}$ in $\mathfrak{M}$, denn es gilt der Satz:

$$\mathfrak{N} \oplus (\mathfrak{M} \ominus \mathfrak{N}) = \mathfrak{M}.$$

Beweis. Daß $\mathfrak{N}$ und $\mathfrak{M} \ominus \mathfrak{N}$ orthogonale Unterräume sind, ist trivial. In $\mathfrak{N}$ gibt es nach § 2, **3** ein in $\mathfrak{N}$ vollständiges Orthonormalsystem $\mathfrak{P}$. Ist $x \in \mathfrak{M}$ beliebig, so ist

$$y = \sum_{\mathfrak{P}} p(x, p) \in \mathfrak{N},$$

weil alle $p \in \mathfrak{N}$ sind, und

$$x - y \in \mathfrak{M} \ominus \mathfrak{N},$$

denn es ist $x - y \in \mathfrak{M}$ und $x - y \perp p$ für alle $p \in \mathfrak{P}$, darum $x - y \perp \sum_{\mathfrak{P}} p(w, p) = w$ für alle $w \in \mathfrak{N}$, $x - y \perp \mathfrak{N}$. Mithin

$$x = y + (x - y) \in \mathfrak{N} \oplus (\mathfrak{M} \ominus \mathfrak{N})$$

für jedes $x \in \mathfrak{M}$. Weil aber andererseits $\mathfrak{N} \subseteqq \mathfrak{M}$ und $\mathfrak{M} \ominus \mathfrak{N} \subseteqq \mathfrak{M}$ ist, folgt die Behauptung [7]).

Ein einfaches Korollar ist der Satz [8]):

Eine Linearmannigfaltigkeit $\mathfrak{M}$ ist entweder in $\mathfrak{R}$ dicht, oder es gibt ein $z \neq 0$ in $\mathfrak{R}$, das auf ganz $\mathfrak{M}$ senkrecht steht.

Beweis. Ist $\widetilde{\mathfrak{M}} = \mathfrak{R}$, so ist $\mathfrak{M}$ in $\mathfrak{R}$ dicht. Andernfalls ist

$$\mathfrak{R} = \widetilde{\mathfrak{M}} \oplus (\mathfrak{R} \ominus \widetilde{\mathfrak{M}}),$$
$$\mathfrak{R} > \widetilde{\mathfrak{M}},$$

darum

$$\mathfrak{R} \ominus \widetilde{\mathfrak{M}} \neq 0.$$

5. Einiger weniger Anwendungen im folgenden wegen wollen wir den Satz von der Existenz eines vollständigen Orthonormalsystems in jedem Raum so verallgemeinern:

Jedem $f \neq 0$ aus $\mathfrak{R}$ sei eine Teilmenge $\mathfrak{M}(f)$ von $\mathfrak{R}$ so zugeordnet, daß folgendes gilt:

1) $f \in \widetilde{\mathfrak{M}(f)}$.

2) *Aus* $\mathfrak{M}(f) \perp g$ *folgt* $\mathfrak{M}(f) \perp \mathfrak{M}(g)$.

Dann gibt es eine Menge $\mathfrak{F}$ aus von 0 verschiedenen Elementen f von $\mathfrak{R}$ so, daß die $\mathfrak{M}(f)$, $f \in \mathfrak{F}$, paarweise orthogonal sind und zusammen $\mathfrak{R}$ als Unterraum erzeugen. (Dann sind natürlich auch die $\widetilde{\mathfrak{M}(f)}$, $f \in \mathfrak{F}$, paarweise orthogonal und der von ihnen erzeugte Unterraum ist $\mathfrak{R}$.)

Beweis (analog § 2, **3**). Wieder sei eine Wohlordnung von $\mathfrak{R}$ gegeben. $\mathfrak{F}$ wird durch transfinite Induktion [4]) erklärt: f werde genau dann in $\mathfrak{F}$ aufgenommen, wenn $f \neq 0$ und $f \perp \mathfrak{M}(g)$ für alle Vorgänger g von f, welche schon in $\mathfrak{F}$ aufgenommen worden sind. Nach 2) sind in dem so konstruierten $\mathfrak{F}$ die $\mathfrak{M}(f)$, $f \in \mathfrak{F}$, paarweise orthogonal. Der von all diesen $\mathfrak{M}(f)$, $f \in \mathfrak{F}$, erzeugte Unterraum heiße $\mathfrak{M}$. Wäre $\mathfrak{M} < \mathfrak{R}$, so gäbe es nach dem soeben bewiesenen Korollar ein $h \neq 0$, das auf $\mathfrak{M}$, d. h. auf allen $\mathfrak{M}(g)$, $g \in \mathfrak{F}$, senkrecht stünde; nach Konstruktion wäre $h \in \mathfrak{F}$, demnach auch $h \perp \mathfrak{M}(h)$, $h \perp \widetilde{\mathfrak{M}(h)}$, nach 1) also $h \perp h$ im Widerspruch mit $h \neq 0$ [9]).

---

[6]) Dies Zeichen wird bei Stone [1] S. 21 in anderem Sinne gebraucht.

[7]) Vgl. Stone [1] S. 23.

[8]) Rieß [2].

[9]) Man kann auch $(\mathfrak{M} \ominus \mathfrak{N}) \oplus \mathfrak{N} = \mathfrak{M}$ direkt beweisen (Rellich [1] S. 344f., Löwig [1] § 2), dann diesen Beweis bringen und aus ihm auf die Existenz eines vollständigen Orthonormalsystems schließen. Dann hat man im ganzen Aufbau nur einen einzigen Wohlordnungsschluß.

6. Es wird sich zeigen, daß die Dimension des Raumes (wird in § 5 definiert) keinen großen Einfluß auf die Operatorentheorie hat, abgesehen davon, daß in endlichdimensionalen Räumen viele Beweise einfacher zu führen sind, weil dort die Mannigfaltigkeit der Operatoren nicht sehr groß ist. Viel wichtiger ist für viele Fragen der Operatorentheorie der Grundkörper Σ des Raumes, und deshalb ist es wohl gerechtfertigt, die Räume nach ihren drei möglichen Grundkörpern verschieden zu benennen, dagegen Eigenschaften wie Separabilität usw. nicht in den Namen der Räume zum Ausdruck zu bringen. Deshalb wollen wir jeden Raum mit $\Sigma = K$ einen *Hilbertschen Raum* nennen, ohne Rücksicht auf seine Dimension. Für Räume mit $\Sigma = R$ hat sich der Name *reeller Hilbertscher Raum* eingebürgert. Ist aber $\Sigma = Q$, so heiße $\mathfrak{R}$ ein *Wachsscher Raum.*

§ 3. Operatoren.

1. Ein *Operator* (linear transformation) A ist eine Funktion, die den x aus einer Linearmannigfaltigkeit $\mathfrak{D} \leqq \mathfrak{R}$ Werte $y = Ax$ aus $\mathfrak{R}$ so zuordnet, daß

$$A(xa + yb) = (Ax)a + (Ay)b,$$

während sie den $x \notin \mathfrak{D}$ nichts zuordnet. $\mathfrak{D}$ heißt der *Definitionsbereich*, die Menge der sinnvollen Ax (d. i. die Menge der Ax, $x \in \mathfrak{D}$) heißt der *Wertebereich von* A. Ist $\mathfrak{D} = \mathfrak{R}$, so heißt A *überall definiert.* A ist *Fortsetzung von* B ($A \geqq B$, $B \leqq A$), wenn aus $y = Bx$ folgt $y = Ax$, d. h. wenn der Definitionsbereich von A den von B enthält und wenn in letzterem A und B an jeder Stelle gleiche Werte annehmen. $A = B$ bedeutet $A \leqq B$ und $B \leqq A$, d. h. Operatoren sind gleich, wenn sie denselben Definitionsbereich haben und in ihm überall gleiche Werte annehmen. Stets ist $A0 = 0$. Ist $\mathfrak{M}$ eine Teilmenge des Definitionsbereichs von A, so sei $A\mathfrak{M}$ die Menge der Ax, $x \in \mathfrak{M}$.

Ist $\lambda \in Z$ (Zentrum von Σ), so gilt identisch

$$(xa + yb)\lambda = (x\lambda)a + (y\lambda)b.$$

Durch

$$\Lambda x = x\lambda$$

wird daher jedem $\lambda \in Z$ ein wohlbestimmter Operator Λ zugeordnet, den wir später mit λE bezeichnen werden. Für $\lambda \in Z$ schreibt man auch

$$\lambda x = x\lambda.$$

Spezialfälle $\lambda = 1$ bzw. $\lambda = 0$ sind: Der Operator, der jedes x sich selbst zuordnet, heiße E; der Operator, der allen Elementen von $\mathfrak{R}$ die 0 zuordnet, werde — ohne Verwechslungsgefahr — 0 geschrieben. Man beachte, daß λx für $\Sigma = Q$, $\lambda \notin \mathfrak{R}$ nicht definiert ist.

2. $A \pm B$, λA ($\lambda \in Z$), AB, $\lim\limits_{n\to\infty} A_n$, A^{-1}, A^* werden wie bei Stone [1] S. 35 ff. definiert: $(A \pm B)x = Ax \pm Bx$, wenn Ax und Bx sinnvoll sind, sonst $(A \pm B)x$ sinnlos; $(\lambda A)x = \lambda(Ax)$, wenn $\lambda \in Z$ und Ax sinnvoll, sonst sinnlos; $(AB)x = A(Bx)$, wenn Bx und $A(Bx)$ sinnvoll sind, sonst sinnlos; $(\lim\limits_{n\to\infty} A_n)x = \lim\limits_{n\to\infty}(A_n x)$, wenn $A_n x$ für alle hinreichend großen n sinnvoll ist und konvergiert, sonst sinnlos; diese Operatoren existieren immer. Wenn aus $Ax = 0$ folgt $x = 0$, so wird A^{-1} so erklärt: A^{-1} ordnet den y aus dem Wertebereich von A das (existierende und eindeutig bestimmte) x mit $Ax = y$ zu ($A^{-1}y = x$), den übrigen y ordnet A^{-1} nichts zu. A^* wird, wenn der Definitionsbereich von A in $\mathfrak{R}$ dicht ist, so erklärt: A^* ordnet den und nur den y etwas zu, zu denen es ein $z \in \mathfrak{R}$ mit

$$(Ax, y) = (x, z)$$

für alle x des Definitionsbereichs von A gibt; dies z ist dann eindeutig bestimmt, und man setzt

$$A^*y = z.$$

Diese Verknüpfungen genügen u. a. folgenden Regeln:

$A + B = B + A.$
$(A + B) + C = A + (B + C).$
$A - B = A + (-1)B.$
$A0 = 0.$
$0A \leqq 0.$
$(AB)C = A(BC).$
$(A \pm B)C = AC \pm BC.$
$A(B \pm C) \geqq AB \pm AC$ (das Zeichen $=$ gilt z. B., wenn A überall definiert ist).
$(\lim_{n\to\infty} A_n)B = \lim_{n\to\infty} (A_nB).$
$(AB)^{-1} = B^{-1}A^{-1}$, wenn A^{-1} und B^{-1} existieren.
Aus $A \leqq B$ folgt $A^* \geqq B^*$, wenn A^* existiert.
$(A \pm B)^* \geqq A^* \pm B^*$, wenn $(A \pm B)^*$ existiert } das Zeichen $=$ gilt z. B.,
$(AB)^* \geqq B^*A^*$, wenn A^* und $(AB)^*$ existieren } wenn A beschränkt ist.
$(\lambda E)^* = \bar{\lambda}E$ $(\lambda \in Z).$
$(A^*)^{-1} = (A^{-1})^*$, wenn A^{-1}, A^* und $(A^{-1})^*$ existieren.

Die Operatoren bilden also keinen Ring.

Das orthogonale Komplement der abgeschlossenen Hülle des Wertebereichs von A ist, wenn A^* existiert, die Menge der x mit $A^*x = 0$.

A heißt abgeschlossen, wenn aus $x_n \to x$, $Ax_n \to y$ folgt, daß Ax sinnvoll und $= y$ ist. A^* ist, wenn vorhanden, immer abgeschlossen.

3. A heißt *stetig*, wenn bei sinnvollen Ax_n und Ax aus $x_n \to x$ stets $Ax_n \to Ax$ folgt. A heißt *beschränkt* (Stone: bounded linear transformation with domain $\mathfrak{R}$), wenn A überall definiert ist und es ein $c \in R$ so gibt, daß

$$|Ax| \leqq c|x|$$

für alle $x \in \mathfrak{R}$ gilt. Dann ist A stetig und A^* ist beschränkt; letzteres beweist man mit folgendem Hilfssatz: Ist jedem $x \in \mathfrak{R}$ ein $f(x) \in \Sigma$ so zugeordnet, daß identisch

$$f(xa + yb) = f(x)a + f(y)b$$

ist und daß aus $x_n \to x$ folgt $f(x_n) \to f(x)$, so gibt es genau ein $g \in \mathfrak{R}$ derart, daß für alle x

$$f(x) = (x, g)$$

gilt [10]). Es gibt unbeschränkte überall definierte Operatoren. Mit A und B sind $A \pm B$, λA $(\lambda \in Z)$, AB beschränkt.

A heißt *hermitesch*, wenn $A \leqq A^*$, *selbstadjungiert* oder *hypermaximal*, wenn $A = A^*$, *nichtnegativ definit* $(A \geqq 0)$, wenn A selbstadjungiert und stets $(Ax, x) \geqq 0$ ist. Beschränkte hermitesche Operatoren sind also von selbst selbstadjungiert. Zu jedem beschränkten und nichtnegativ definiten Operator M gibt es einen ebensolchen Operator N mit $M = N^2$, und ist C beschränkt, $CM = MC$, so folgt $CN = NC$ [11]).

Ein *Projektor* (Einzel-, Projektionsoperator, projection) ist ein beschränkter hermitescher Operator P mit $P^2 = P$. Sein Wertebereich $\mathfrak{M}$ ist Unterraum, und für $x \in \mathfrak{M}$ ist $Px = x$, für $x \in \mathfrak{R} \ominus \mathfrak{M}$ ist $Px = 0$. Ist umgekehrt $\mathfrak{M}$ ein Unterraum, so ist der Operator, der jedem $x \in \mathfrak{R}$ das $y \in \mathfrak{M}$ mit $x - y \perp \mathfrak{M}$ (§ 2, **4**) zuordnet, ein Projektor;

[10]) Rellich [1] S. 345f., Löwig [1] S. 11f., Rieß [2] S. 37f.
[11]) Wecken [1].

so hat man eine eindeutige Beziehung zwischen der Menge aller Projektoren und der Menge aller Unterräume. P und Q seien Projektoren, $\mathfrak{M}$ und $\mathfrak{N}$ die zugehörigen Unterräume. Dann ist $PQ = QP$ dann und nur dann, wenn $P\mathfrak{N} \leq \mathfrak{N}$ (oder $Q\mathfrak{M} \leq \mathfrak{M}$). Und zwar ist dann PQ der zu $\mathfrak{M} \cap \mathfrak{N}$ gehörige Projektor; ist $\mathfrak{M} \geqq \mathfrak{N}$, so ist $P - Q$ der zu $\mathfrak{M} \ominus \mathfrak{N}$ gehörende Projektor, und ist $\mathfrak{M} \perp \mathfrak{N}$, so ist $P + Q$ der zu $\mathfrak{M} \oplus \mathfrak{N}$ gehörende Projektor.

Eine „isomorphe" Abbildung zweier Linearmannigfaltigkeiten aufeinander, eine Abbildung $x \to Ux$ also mit den Eigenschaften

$$U(x + y) = Ux + Uy,$$
$$U(xa) = (Ux)a,$$
$$(Ux, Uy) = (x, y),$$

ist ein *isometrischer Operator*. Ist $\mathfrak{R}$ Definitions- und Wertebereich, so heißt U *unitär*. Die unitären Operatoren sind genau die beschränkten Operatoren U mit

$$U^*U = UU^* = E.$$

Zwei Operatoren A und B heißen *unitäräquivalent*, wenn es ein unitäres U mit

$$UAU^{-1} = B$$

gibt [12]).

4. Die Menge der Paare $\{x, y\}$, $x \in \mathfrak{R}$, $y \in \mathfrak{R}$, bildet bei der Verknüpfung

$$\{x, y\} + \{x', y'\} = \{x + x', y + y'\}$$
$$\{x, y\}a = \{xa, ya\}$$
$$(\{x, y\}, \{x', y'\}) = (x, x') + (y, y')$$

einen Raum, den wir $\mathfrak{R}^2$ nennen wollen. In ihm erklären wir die Operatoren V und F durch

$$V\{x, y\} = \{y, -x\},$$
$$F\{x, y\} = \{x, 0\}.$$

Dann ist $V^2 = -\bar{E}$, $V^* = -V$, V unitär, F Projektor. Den Wertebereich $F\mathfrak{R}^2$ von F, die Menge der $\{x, 0\}$ $(x \in \mathfrak{R})$, nennen wir den Abszissenraum, sein orthogonales Komplement $(\bar{E} - F)\mathfrak{R}^2$, die Menge der $\{0, y\}$ $(y \in \mathfrak{R})$, den Ordinatenraum.

Jedem Operator A in $\mathfrak{R}$ wird durch

$$\bar{A}\{x, y\} = \{Ax, Ay\}, \text{ wenn } Ax \text{ und } Ay \text{ sinnvoll sind,}$$
$$\bar{A}\{x, y\} \text{ sonst sinnlos}$$

ein Operator $\bar{A}$ in $\mathfrak{R}^2$ so zugeordnet, daß

$$\overline{(A \pm B)} = \bar{A} \pm \bar{B}.$$
$$\overline{(\lambda A)} = \lambda \bar{A} \quad (\lambda \in Z).$$
$$\overline{(AB)} = \bar{A}\bar{B}.$$
$$\overline{\lim_{n\to\infty} A_n} = \lim_{n\to\infty} \bar{A}_n.$$
$$\left.\begin{aligned} \bar{A}^{-1} &= \overline{A^{-1}} \\ \bar{A}^* &= \overline{A^*} \end{aligned}\right\} \text{ wenn eine der beiden Seiten existiert.}$$

Ferner wird jedem Operator A von $\mathfrak{R}$ als Bild $\mathfrak{B}_A$ die Menge aller $\{x, Ax\}$ zugeordnet, wo x den Definitionsbereich von A durchläuft. Dies ist eine eineindeutige Abbildung der Menge aller Operatoren von $\mathfrak{R}$ auf die Menge aller derjenigen Linearmannigfaltigkeiten in $\mathfrak{R}^2$, die mit dem Ordinatenraum den Durchschnitt 0 haben (d. h. die sich eindeutig in den Abszissenraum projizieren). Insbesondere ist jede Linearmannigfaltigkeit, die im Bild eines Operators enthalten ist, selbst Bild eines Operators.

[12]) Stone [1] S. 49—85.

$A \leqq B$ ist gleichbedeutend mit $\mathfrak{B}_A \leqq \mathfrak{B}_B$. A ist genau dann abgeschlossen, wenn $\mathfrak{B}_A$ abgeschlossen (d. h. Unterraum) ist.

A sei ein abgeschlossener Operator. Dann existiert A^* dann und nur dann, wenn $\mathfrak{R}^2 \ominus V\mathfrak{B}_A$ Bild eines Operators ist, und zwar ist dann

$$\mathfrak{B}_{A^*} = \mathfrak{R}^2 \ominus V\mathfrak{B}_A .$$

Beweis. Die Gleichung

$$(Ax, y) = (x, z)$$

ist mit

$$(\{y, z\}, V\{x, Ax\}) = 0$$

gleichwertig, wie man sofort sieht. Existiert also A^*, so sind $\{y, z\} \in \mathfrak{B}_{A^*}$ und $\{y, z\} \perp V\mathfrak{B}_A$ gleichwertig. Und A^* existiert genau dann, wenn oben z durch y eindeutig bestimmt ist; das ist aber genau dann der Fall, wenn es kein $\{0, z\} \neq 0$ in $\mathfrak{R}^2 \ominus V\mathfrak{B}_A$ gibt, d. h. wenn $\mathfrak{R}^2 \ominus V\mathfrak{B}_A$ Bild eines Operators ist.

Ist A abgeschlossen und A^* vorhanden, so folgt durch Anwenden des unitären Operators V auf

$$\mathfrak{R}^2 = \mathfrak{B}_{A^*} \oplus V\mathfrak{B}_A ,$$

weil $V^2 = -\overline{E}$ und darum $V^2\mathfrak{B}_A = \mathfrak{B}_A$ ist, daß

$$\mathfrak{R}^2 = V\mathfrak{B}_{A^*} \oplus \mathfrak{B}_A ,$$

daher $A^{**} = A$. Unter denselben Voraussetzungen ist

$$(A^*A + E)^{-1} = H$$

ein beschränkter hermitescher Operator mit $(Hx, x) > 0$ $(x \neq 0)$ [13]).

§ 4. Vertauschbarkeit.

1. Nachdem wir nun die wichtigsten grundlegenden Definitionen und Sätze ohne Mühe in unsere allgemeinen Räume übertragen haben, soll, bevor Neues in Angriff genommen wird, das Wichtigste über den von v. Neumann [2] und Rieß [1] gebrauchten Vertauschbarkeitsbegriff zusammengestellt werden. Ich halte es für aussichtlos, die Vertauschbarkeit allgemeiner, als es hier geschieht, in vernünftiger Weise definieren zu wollen.

Wir schreiben

$$C \mathfrak{v} A ,$$

wenn C beschränkt ist und

$$CA \leqq AC$$

gilt.

Aus $C\mathfrak{v}A$ und $C\mathfrak{v}B$ folgt $C\mathfrak{v}A \pm B$ und $C\mathfrak{v}AB$.

Beweis. $C(A \pm B) = CA \pm CB \leqq AC \pm BC = (A \pm B)C,$

$$CAB \leqq ACB \leqq ABC.$$

Aus $C\mathfrak{v}A$ und $D\mathfrak{v}A$ folgt $C \pm D\mathfrak{v}A$ und $CD\mathfrak{v}A$.

Beweis. $(C \pm D)\,A = CA \pm DA \leqq AC \pm AD \leqq A(C \pm D),$

$$CDA \leqq CAD \leqq ACD.$$

$\lambda E \mathfrak{v} A$ $(\lambda \in Z)$ gilt allgemein. Sind A und B beschränkt, so sind $A\mathfrak{v}B$ und $B\mathfrak{v}A$ gleichbedeutend.

Existiert A^{-1}, so folgt aus $C\mathfrak{v}A$, daß $C\mathfrak{v}A^{-1}$.

Beweis. Es ist zu zeigen, daß dann aus der Existenz von $CA^{-1}x$ folgt, daß $A^{-1}Cx$

[13]) v. Neumann [3] bis S. 302.

existiert und $= CA^{-1}x$ ist. Existiert $CA^{-1}x$, so existiert (nach Definition des Operatorenproduktes) $A^{-1}x$, nach Definition von A^{-1} ist $x = AA^{-1}x$, daher

$$Cx = CAA^{-1}x = ACA^{-1}x,$$

letzteres wegen $CA \leqq AC$ (Vor.). Cx liegt demnach im Wertebereich von A, $A^{-1}Cx$ existiert, und es ist

$$A^{-1}Cx = CA^{-1}x.$$

Aus $C \mathfrak{v} A_n (n = 1, 2, \ldots)$ *folgt* $C \mathfrak{v} \lim_{n\to\infty} A_n$.

Beweis. Existiert $C \lim_{n\to\infty} A_n x$, so ist $A_n x$ für hinreichend große n sinnvoll und konvergent; wegen der Stetigkeit von C und wegen $C \mathfrak{v} A_n$ gilt

$$C \lim A_n x = \lim CA_n x = \lim (A_n Cx) = (\lim A_n) Cx.$$

Gilt $C_n \mathfrak{v} A$, *ist* $\lim C_n$ *ein beschränkter Operator und ist* A *abgeschlossen, so gilt* $\lim C_n \mathfrak{v} A$.

Beweis. Ist Ax sinnvoll, so konvergieren $\lim C_n x$ und $\lim AC_n x$ (weil $AC_n x = C_n Ax$ ist); wegen der Abgeschlossenheit von A folgt, daß auch $A \lim C_n x$ existiert und

$$A \lim C_n x = \lim AC_n x = \lim C_n Ax$$

ist.

Die interessanteste dieser Regeln ist aber diese:

Wenn A^* *existiert, so folgt aus* $C \mathfrak{v} A$, *daß* $C^* \mathfrak{v} A^*$.

Beweis. Dann ist der Definitionsbereich von CA gleich dem von A, also in $\mathfrak{R}$ dicht, $(CA)^*$ existiert. Wegen $CA \leqq AC$ ist erst recht der Definitionsbereich von AC in $\mathfrak{R}$ dicht, $(AC)^*$ existiert, und es ist

$$(AC)^* \leqq (CA)^*.$$

Nach der Regel über den zu einem Produkt adjungierten Operator aus § 3, 2 folgt (C ist ja beschränkt)

$$C^*A^* \leqq (AC)^* \leqq (CA)^* = A^*C^*.$$

Hieraus folgt: Existiert noch A^{**}, so gilt

$$C = C^{**} \mathfrak{v} A^{**}.$$

2. Es sei $\mathfrak{R} = \mathfrak{M} \oplus \mathfrak{N}$ (in dieser Formel ist enthalten, daß $\mathfrak{M}$ und $\mathfrak{N}$ orthogonale Unterräume sind, von denen jeder das orthogonale Komplement des andern ist). In $\mathfrak{M}$ sei ein Operator A_1 mit dem Definitionsbereich $\mathfrak{D}_1$ gegeben, dessen Wertebereich natürlich in $\mathfrak{M}$ enthalten sein muß. Analog A_2 mit dem Definitionsbereich $\mathfrak{D}_2$ in $\mathfrak{N}$. Dann können wir uns auf folgende einfache Weise einen Operator in $\mathfrak{R}$ bauen: Als Definitionsbereich $\mathfrak{D}$ nehmen wir $\mathfrak{D}_1 \dot{+} \mathfrak{D}_2$ (der Durchschnitt von $\mathfrak{D}_1 \leqq \mathfrak{M}$ und $\mathfrak{D}_2 \leqq \mathfrak{N}$ ist ja 0), und ist $x = y + z$, $x \in \mathfrak{D}$, $y \in \mathfrak{D}_1$, $z \in \mathfrak{D}_2$, so setzen wir

$$Ax = A_1 y + A_2 z.$$

Nun kann man sich umgekehrt fragen, ob ein gegebener Operator A als auf solche Weise entstanden gedacht werden kann. So kommt man zu der

Definition. A sei ein Operator in $\mathfrak{R}$ mit dem Definitionsbereich $\mathfrak{D}$, $\mathfrak{M}$ sei ein Unterraum von $\mathfrak{R}$. Wir sagen, $\mathfrak{M}$ reduziert A, wenn es Linearmannigfaltigkeiten $\mathfrak{D}_1 \leqq \mathfrak{M}$ und $\mathfrak{D}_2 \leqq \mathfrak{R} \ominus \mathfrak{M}$ so gibt, daß folgende drei Bedingungen erfüllt sind:

1. A nimmt in $\mathfrak{D}_1$ nur Werte aus $\mathfrak{M}$ an.
2. A nimmt in $\mathfrak{D}_2$ nur Werte aus $\mathfrak{R} \ominus \mathfrak{M}$ an.
3. $\mathfrak{D} = \mathfrak{D}_1 \dot{+} \mathfrak{D}_2$.

Sind diese Bedingungen erfüllt, so ist natürlich $\mathfrak{D}_1 = \mathfrak{D} \cap \mathfrak{M}$ und $\mathfrak{D}_2 = \mathfrak{D} \cap (\mathfrak{R} \ominus \mathfrak{M})$. Ist noch P der zu $\mathfrak{M}$ gehörige Projektor, also $\mathfrak{M}$ der Wertebereich von P und $\mathfrak{R} \ominus \mathfrak{M}$

der Wertebereich von $E - P$, so kann man bei Beachtung dieser Bemerkung die notwendigen und hinreichenden Bedingungen dafür, daß $\mathfrak{M}$ den Operator reduziert, auch in folgender Form schreiben:

1. $AP = PAP$.
2. $A(E - P) = (E - P)\,A(E - P)$.
3. $A = AP + A(E - P)$ [14]).

In der Tat: 1. besagt, daß die Werte, die A an Stellen annimmt, die in der Form Px geschrieben werden können (d. h. die in $\mathfrak{M}$ liegen), bei Anwendung von P ungeändert bleiben, also gleichfalls in $\mathfrak{M}$ liegen, folglich nimmt A im Durchschnitt seines Definitionsbereichs mit $\mathfrak{M}$ nur Werte aus $\mathfrak{M}$ an. Entsprechend besagt 2., daß A in $\mathfrak{D} \cap (\mathfrak{R} \ominus \mathfrak{M})$ nur Werte aus $\mathfrak{R} \ominus \mathfrak{M}$ annimmt. Und schließlich besagt 3., daß mit x stets auch Px und $(E - P)x$ im Definitionsbereich von A liegen, d. h.

$$\mathfrak{D} = (\mathfrak{D} \cap \mathfrak{M}) \dotplus (\mathfrak{D} \cap (\mathfrak{R} \ominus \mathfrak{M})).$$

Diese drei Gleichungen sind nun aber mit

$$P \mathfrak{v} A$$

gleichwertig. Denn sind jene erfüllt, so ist

$$PA = P(AP + A(E - P)) = P(AP + (E - P)\,A(E - P)) = PAP + 0A(E - P)$$
$$= AP + 0A(E - P) \leqq AP.$$

Umgekehrt sei $P \mathfrak{v} A$ erfüllt. Dann ist

$$PAP \leqq AP^2 = AP;$$

weil aber beide Seiten denselben Definitionsbereich haben, gilt sogar

$$PAP = AP.$$

Aus $E \mathfrak{v} A$ und $P \mathfrak{v} A$ folgt $(E - P) \mathfrak{v} A$, und weil auch $E - P$ Projektor ist, gilt entsprechend

$$(E - P)A(E - P) = A(E - P).$$

Schließlich folgt

$$A = PA + (E - P)A \leqq AP + A(E - P),$$

darum [14])

$$A = AP + A(E - P)$$ [15]).

Zusatz. Ist C beschränkt und führen C und C^* den Unterraum $\mathfrak{M}$ in eine Teilmenge von $\mathfrak{M}$ über, so reduziert $\mathfrak{M}$ den Operator C [16]).

3. Wir haben in § 3, **4** den Operatoren A in $\mathfrak{R}$ Operatoren $\overline{A}$ in $\mathfrak{R}^2$ zugeordnet. Ferner führten wir V und F ein. Es gilt

$$V \mathfrak{v} \overline{A} \quad \text{und} \quad F \mathfrak{v} \overline{A}.$$

Denn ist $\overline{A}\{x, y\}$ sinnvoll, d. h. sind Ax und Ay sinnvoll, so ist

$$V\overline{A}\{x, y\} = \{Ay, -Ax\} = \overline{A}\,V\{x, y\},$$
$$F\overline{A}\{x, y\} = \{Ax, 0\} = \overline{A}F\{x, y\}.$$

Es gilt aber auch die Umkehrung, nämlich:

Ist D ein Operator in $\mathfrak{R}^2$, gilt $V \mathfrak{v} D$ und $F \mathfrak{v} D$, so gibt es einen Operator A in $\mathfrak{R}$ mit $\overline{A} = D$.

Beweis. F ist der zum Abszissenraum gehörige Projektor, aus $F \mathfrak{v} D$ folgt darum, daß D in der zu Anfang von § 4, **2** erklärten Weise aus einem Operator im Abszissenraum und einem Operator im Ordinatenraum zusammengebaut ist: Es gibt Operatoren

[14]) $A \geqq AP + A(E - P)$ gilt identisch.

[15]) In anderer Form s. v. Neumann [1] IV.

[16]) Stone [1] S. 152.

A und B in $\mathfrak{R}$ so, daß

$$D\{x, y\} = \{Ax, By\},$$

wenn Ax und By sinnvoll sind, und $D\{x, y\}$ sonst sinnlos ist. Denn jeder Operator im Abszissenraum ist ja eine Transformation

$$\{x, 0\} \to \{Ax, 0\}$$

bei passendem Operator A in $\mathfrak{R}$; entsprechend für den Ordinatenraum. Aus $V \mathfrak{v} D$ folgt nun

$$\{By, -Ax\} = VD\{x, y\} = DV\{x, y\} = \{Ay, -Bx\},$$

sowie Ax und By sinnvoll sind. Vergleich der Abszissen liefert $B \leqq A$, Vergleich der Ordinaten liefert $A \leqq B$, zusammen $A = B$. Damit ist die Behauptung bewiesen.

Ist $\mathfrak{B}_A$ das A in § 3. 4 *zugeordnete Bild und C beschränkt, so ist $C \mathfrak{v} A$ gleichwertig mit*

$$\bar{C}\mathfrak{B}_A \leqq \mathfrak{B}_A.$$

Beweis. $C \mathfrak{v} A$ bedeutet, daß, sowie Ax sinnvoll ist,

$$CAx = ACx$$

ist; dies ist gleichbedeutend damit, daß, sowie Ax sinnvoll ist,

$$\{Cx, CAx\} = \bar{C}\{x, Ax\}$$

zu $\mathfrak{B}_A$ gehört, und letzteres besagt genau $\bar{C}\mathfrak{B}_A \leqq \mathfrak{B}_A$ [17]).

§ 5. Die Dimension [17a]).

1. Löwig definiert [18]) die Dimension einer Linearmannigfaltigkeit $\mathfrak{L}$ in $\mathfrak{R}$ als die Mächtigkeit eines vollständigen Orthonormalsystems in $\tilde{\mathfrak{L}}$, die, wie er beweist, von der speziellen Wahl des Orthonormalsystems unabhängig ist. Er fängt aber mit seiner Definition nichts an, sondern rechtfertigt damit nur die Überschrift seiner Arbeit. Wir wollen hier, von einer im Wortlaut etwas anderen und ohne vorherigen Existenz- und Eindeutigkeitssatz auskommenden Definition ausgehend, in zwei Abschnitten eine ausführliche Diskussion dieses Begriffs geben.

Unter einer *Grundmenge* $\mathfrak{G}$ in der Linearmannigfaltigkeit $\mathfrak{L}$ verstehen wir [19]) eine Teilmenge von $\mathfrak{L}$ mit der Eigenschaft, daß die davon erzeugte Linearmannigfaltigkeit $\widehat{\mathfrak{G}}$ in $\mathfrak{L}$ dicht ist, oder, was dasselbe ist,

$$\mathfrak{G} \leqq \mathfrak{L} \leqq \tilde{\mathfrak{G}}.$$

Haupteigenschaften dieses Begriffs sind:

Sind die $\mathfrak{L}_\nu$ Linearmannigfaltigkeiten (ν durchläuft eine beliebige Menge von Indizes), ist $\mathfrak{G}_\nu$ für jedes ν eine Grundmenge in $\mathfrak{L}_\nu$ und sind alle $\mathfrak{L}_\nu$ zusammengenommen eine Grundmenge in der Linearmannigfaltigkeit $\mathfrak{M}$, so sind auch alle $\mathfrak{G}_\nu$ zusammen schon eine Grundmenge in $\mathfrak{M}$. Man beachte den Spezialfall, daß nur ein einziges $\mathfrak{L}_\nu$ vorgelegt ist.

Ist $\mathfrak{G}$ Grundmenge in $\mathfrak{L}$ und ist A ein stetiger Operator, dessen Definitionsbereich $\mathfrak{L}$ enthält, so ist auch $A\mathfrak{G}$ Grundmenge in $A\mathfrak{L}$.

Bekanntlich gibt es in jeder nichtleeren Menge von Kardinalzahlen eine kleinste. Die Menge der Mächtigkeiten aller Grundmengen in einer gegebenen Linearmannigfaltigkeit $\mathfrak{L}$ ist nicht leer, denn es gibt Grundmengen in $\mathfrak{L}$ (z. B. $\mathfrak{L}$ selbst). Daher dürfen wir definieren:

---

[17]) Warnung: Dieser Satz eignet sich nicht zu einer Verallgemeinerung des Vertauschbarkeitsbegriffs.

[17a]) Zus. b. d. Korr. Inzwischen hat H. Löwig in einer Arbeit: „*Über die Dimension linearer Räume*", Studia math. **5** (1935), 18—23 ähnliche Ergebnisse gewonnen.

[18]) Löwig [1] S. 32.

[19]) Mit geringer Abweichung von Hausdorff [1] S. 295.

Die Dimension einer Linearmannigfaltigkeit $\mathfrak{L}$ (geschrieben Dim $\mathfrak{L}$) ist die kleinste unter den Mächtigkeiten aller Grundmengen in $\mathfrak{L}$.

2. Die von endlich vielen Elementen von $\mathfrak{R}$ erzeugte Linearmannigfaltigkeit ist stets ein Unterraum [20]). Hieraus folgt:

Gibt es in $\mathfrak{L}$ eine Grundmenge, die nur aus n Elementen ($n < \infty$) besteht, so ist $\mathfrak{L}$ der von diesen n Elementen erzeugte Σ-Rechtsmodul, also höchstens vom Rang n. Umgekehrt gilt trivialerweise: Ist $\mathfrak{L}$ ein Σ-Rechtsmodul vom Rang $n < \infty$, so gibt es in $\mathfrak{L}$ eine Grundmenge von n Elementen (nämlich eine Basis). Zusammengenommen:

Dim $\mathfrak{L}$ *hat genau dann den endlichen Wert* n, *wenn* $\mathfrak{L}$ *ein* Σ*-Rechtsmodul vom Rang* n *ist.*

Und setzt man, wie im folgenden stets,

$$\sum_{\nu=0}^{\infty} 1 = \mathfrak{a},$$

so ist $\mathfrak{L}$ *dann und nur dann separabel, wenn* Dim $\mathfrak{L} \leqq \mathfrak{a}$ *ist* [21]).

3. Ist A ein stetiger Operator, dessen Definitionsbereich die Linearmannigfaltigkeit $\mathfrak{L}$ enthält, so ist

$$\text{Dim } A\mathfrak{L} \leqq \text{Dim } \mathfrak{L}.$$

Denn die Dimension von $A\mathfrak{L}$ ist nicht größer als die Mächtigkeit der Grundmenge $A\mathfrak{G}$ von $A\mathfrak{L}$, wo für $\mathfrak{G}$ eine beliebige Grundmenge von $\mathfrak{L}$ — auch eine solche mit der Mächtigkeit Dim $\mathfrak{L}$ — eingesetzt werden darf. Abschätzungen in umgekehrter Richtung werden wir erst in § 6 gewinnen.

Eins aber sieht man jetzt schon:

Sind $\mathfrak{L}$ *und* $\mathfrak{M}$ *zwei separable Linearmannigfaltigkeiten, die eineindeutig linear aufeinander abgebildet sind, so ist*

$$\text{Dim } \mathfrak{L} = \text{Dim } \mathfrak{M}.$$

Beweis. Hat $\mathfrak{L}$ die endliche Dimension n, so auch $\mathfrak{M}$, weil dann $\mathfrak{L}$ und $\mathfrak{M}$ beide endliche Σ-Rechtsmoduln vom Rang n sind. Dasselbe gilt, wenn $\mathfrak{M}$ endliche Dimension hat. Sind aber Dim $\mathfrak{L}$ und Dim $\mathfrak{M}$ beide unendlich, so sind sie auch gleich, nämlich beide $= \mathfrak{a}$.

4. $\mathfrak{L}$ *und* $\mathfrak{M}$ *seien Linearmannigfaltigkeiten,* $\mathfrak{L} \leqq \mathfrak{M}$, $\mathfrak{L}$ *in* $\mathfrak{M}$ *dicht* (*z. B.* $\mathfrak{M} = \tilde{\mathfrak{L}}$). *Dann ist*

$$\text{Dim } \mathfrak{L} = \text{Dim } \mathfrak{M}.$$

Beweis. Ist Dim $\mathfrak{M} < \mathfrak{a}$, so ist $\mathfrak{L}$ Unterraum; aus

$$\mathfrak{L} \leqq \mathfrak{M} \leqq \tilde{\mathfrak{L}} = \mathfrak{L}$$

folgt also $\mathfrak{L} = \mathfrak{M}$, Dim $\mathfrak{L} =$ Dim $\mathfrak{M}$. Es sei also Dim $\mathfrak{M} \geqq \mathfrak{a}$. Dann ist einerseits jede Grundmenge in $\mathfrak{L}$ auch Grundmenge in $\mathfrak{M}$, also Dim $\mathfrak{L} \geqq$ Dim $\mathfrak{M}$. Ist andererseits $\mathfrak{G}$ eine Grundmenge in $\mathfrak{M}$ von der Mächtigkeit Dim $\mathfrak{M}$, so wähle man zu jedem $g \in \mathfrak{G}$ eine Folge $f_n \in \mathfrak{L}$ mit $\lim_{n\to\infty} f_n = g$ aus und bezeichne die Menge all dieser f_n mit $\mathfrak{F}$; dann hat $\mathfrak{F}$ höchstens die Mächtigkeit

$$\mathfrak{a}\,\text{Dim } \mathfrak{M} = \text{Dim } \mathfrak{M},$$

und wegen

$$\mathfrak{F} \leqq \mathfrak{L} \leqq \mathfrak{M} \leqq \mathfrak{G} \leqq \tilde{\mathfrak{F}}$$

---

[20]) Hausdorff [1] S. 298.

[21]) Vgl. Hausdorff [1] S. 295f.

ist $\mathfrak{F}$ Grundmenge in $\mathfrak{L}$, deshalb

$$\text{Dim } \mathfrak{L} \leqq \text{Dim } \mathfrak{M}\ ^{22})\ ^{23}).$$

5. *Die $\mathfrak{L}_\nu$ seien paarweise orthogonale Linearmannigfaltigkeiten, deren Vereinigungsmenge Grundmenge in der Linearmannigfaltigkeit $\mathfrak{L}$ sei; ν durchläuft eine beliebige Menge von Indizes. Dann ist*

$$\text{Dim } \mathfrak{L} = \sum_\nu \text{Dim } \mathfrak{L}_\nu .$$

Beweis. Es sei $\mathfrak{S}_\nu$ der von $\mathfrak{L}_\nu$, $\mathfrak{S}$ der von $\mathfrak{L}$ erzeugte Unterraum. Dann sind die $\mathfrak{S}_\nu$ paarweise orthogonale Unterräume, die zusammen den Unterraum $\mathfrak{S}$ erzeugen, und nach dem eben Bewiesenen ist

$$\text{Dim } \mathfrak{L}_\nu = \text{Dim } \mathfrak{S}_\nu ,$$
$$\text{Dim } \mathfrak{L} = \text{Dim } \mathfrak{S} ;$$

die Behauptung reduziert sich also auf

$$\text{Dim } \mathfrak{S} = \sum_\nu \text{Dim } \mathfrak{S}_\nu .$$

Ist Dim $\mathfrak{S}$ endlich, so ist $\mathfrak{S}$ die direkte Summe der endlichen Σ-Rechtsmoduln $\mathfrak{S}_\nu$, und alles ist klar. Sei also Dim $\mathfrak{S}$ unendlich. Ist dann $\mathfrak{G}_\nu$ eine Grundmenge in $\mathfrak{S}_\nu$, so bilden alle $\mathfrak{G}_\nu$ zusammen eine Grundmenge in $\mathfrak{S}$, daher

$$\text{Dim } \mathfrak{S} \leqq \sum_\nu \text{Dim } \mathfrak{S}_\nu .$$

Umgekehrt sei $\mathfrak{G}$ eine Grundmenge in $\mathfrak{S}$ mit der Mächtigkeit Dim $\mathfrak{S}$. P_ν sei der zu $\mathfrak{S}_\nu$ gehörige Projektor. Dann werde $\mathfrak{G}_\nu$ definiert als $P_\nu \mathfrak{G}$, wo aus $P_\nu \mathfrak{G}$ aber die Nullen weggelassen werden sollen. Wegen der Orthogonalität der $\mathfrak{S}_\nu$ gilt die Gleichung

$$|g|^2 = \sum_\nu |P_\nu g|^2$$

für alle $g \in \mathfrak{G}$, zu jedem $g \in \mathfrak{G}$ gibt es also höchstens abzählbar viele ν mit $P_\nu g \neq 0$. Ist $\mathfrak{d}_\nu$ die Mächtigkeit von $\mathfrak{G}_\nu$, so folgt

$$\sum_\nu \mathfrak{d}_\nu \leqq \mathfrak{a}\ \text{Dim } \mathfrak{S} = \text{Dim } \mathfrak{S}.$$

Andererseits ist P_ν ein stetiger Operator; weil nun $\mathfrak{G}$ Grundmenge in $\mathfrak{S}$ ist, muß $P_\nu \mathfrak{G}$ Grundmenge in $P_\nu \mathfrak{S}$ sein, d. h. $\mathfrak{G}_\nu$ ist Grundmenge in $\mathfrak{S}_\nu$, hieraus folgt

$$\text{Dim } \mathfrak{S}_\nu \leqq \mathfrak{d}_\nu ,$$

mithin

$$\sum_\nu \text{Dim } \mathfrak{S}_\nu \leqq \sum_\nu \mathfrak{d}_\nu \leqq \text{Dim } \mathfrak{S}.$$

6. Dieser Satz gestattet viele Anwendungen.

$\mathfrak{P}$ sei ein vollständiges Orthonormalsystem in der Linearmannigfaltigkeit $\mathfrak{L}$, d. h. das Orthonormalsystem $\mathfrak{P} < \mathfrak{L}$ habe die Eigenschaft, daß für alle $x \in \mathfrak{L}$ gilt

$$x = \sum_{\mathfrak{P}} p(x, p).$$

Dann ist die Dimension von $\mathfrak{L}$ gleich der Mächtigkeit von $\mathfrak{P}$.

Beweis. Ordnet man jedem $p \in \mathfrak{P}$ den von p allein erzeugten Unterraum $\mathfrak{L}_p$ zu, so erfüllen die $\mathfrak{L}_p$ und $\mathfrak{L}$ die Voraussetzungen des eben bewiesenen Satzes, und alle $\mathfrak{L}_p$ haben die Dimension 1. Daher

$$\text{Dim } \mathfrak{L} = \sum_{\mathfrak{P}} 1.$$

Rechts steht aber gerade die Mächtigkeit von $\mathfrak{P}$. Hiermit ist die Übereinstimmung unseres Dimensionsbegriffs mit dem Löwigschen nachgewiesen und zugleich gezeigt,

---

[22]) Bis hierher gilt alles in beliebigen linearen metrischen Räumen.

[23]) Jetzt kann man die Übereinstimmung unserer Dimension mit Löwigs Dimension so einsehen: Es genügt, das Übereinstimmen für Unterräume zu zeigen. Einerseits ist aber jedes vollständige Orthonormalsystem eine Grundmenge, andererseits stellt das von Rellich [1] S. 356 angewandte Orthogonalisierungsverfahren aus jeder Grundmenge ein vollständiges Orthonormalsystem von nicht höherer Mächtigkeit her.

daß alle in derselben Linearmannigfaltigkeit vollständigen Orthonormalsysteme gleiche Mächtigkeit haben.

$\mathfrak{S}$ sei ein Unterraum, und die $\mathfrak{d}_\nu$ seien Kardinalzahlen mit der Eigenschaft

$$\mathrm{Dim}\,\mathfrak{S} = \sum_\nu \mathfrak{d}_\nu.$$

Dann gibt es paarweise orthogonale Unterräume $\mathfrak{S}_\nu$ in $\mathfrak{S}$ mit den Dimensionen

$$\mathrm{Dim}\,\mathfrak{S}_\nu = \mathfrak{d}_\nu,$$

die zusammen $\mathfrak{S}$ als Unterraum erzeugen.

Beweis. $\mathfrak{P}$ sei ein vollständiges Orthonormalsystem in $\mathfrak{S}$, also von der Mächtigkeit Dim $\mathfrak{S}$. Dann gibt es jedenfalls eine Zerlegung von $\mathfrak{P}$ in paarweise fremde Teilmengen $\mathfrak{P}_\nu$ von der Mächtigkeit $\mathfrak{d}_\nu$. Für $\mathfrak{S}_\nu$ kann man den von $\mathfrak{P}_\nu$ erzeugten Unterraum nehmen.

Zwei Unterräume $\mathfrak{S}$ und $\mathfrak{T}$ mögen dieselbe Dimension haben. Dann kann man den einen durch einen isometrischen Operator auf den andern abbilden. Sind nämlich $\mathfrak{P}$ und $\mathfrak{Q}$ vollständige Orthonormalsysteme in $\mathfrak{S}$ bzw. $\mathfrak{T}$, so kann man jedenfalls die gleichmächtigen Mengen $\mathfrak{P}$ und $\mathfrak{Q}$ eineindeutig aufeinander abbilden. Es ist leicht zu sehen, daß sich diese eineindeutige Abbildung eindeutig zu einer isometrischen Abbildung von $\mathfrak{S}$ auf $\mathfrak{T}$ fortsetzen läßt.

Sind $\mathfrak{L}$ und $\mathfrak{M}$ zwei Linearmannigfaltigkeiten mit $\mathfrak{L} \leqq \mathfrak{M}$, so ist

$$\mathrm{Dim}\,\mathfrak{L} \leqq \mathrm{Dim}\,\mathfrak{M}.$$

Beweis. $\mathrm{Dim}\,\mathfrak{L} = \mathrm{Dim}\,\tilde{\mathfrak{L}} \leqq \mathrm{Dim}\,\tilde{\mathfrak{L}} + \mathrm{Dim}\,(\tilde{\mathfrak{M}} \ominus \tilde{\mathfrak{L}}) = \mathrm{Dim}\,\tilde{\mathfrak{M}} = \mathrm{Dim}\,\mathfrak{M}.$

§ 6. Weitere Sätze über die Dimension.

1. In diesem Abschnitt sollen einige Sätze über das Verhalten der Dimension bei Abbildungen und das Additionstheorem bewiesen werden, die in separablen Räumen trivial sind, die aber im allgemeinen Fall nicht ganz so einfach wie die Ergebnisse des vorigen Abschnitts sind. Die Quelle all dieser Sätze ist folgende Tatsache:

A sei ein stetiger Operator, dessen Definitionsbereich das Orthonormalsystem $\mathfrak{P}$ enthält. Dann kann man $\mathfrak{P}$ so in höchstens abzählbar unendliche Klassen zerlegen, daß, sowie $p \in \mathfrak{P}$ und $q \in \mathfrak{P}$ in verschiedenen Klassen liegen, $Ap \perp Aq$ gilt.

Beweis. Unter einer $p \in \mathfrak{P}$ und $q \in \mathfrak{P}$ verbindenden Kette verstehen wir für den Augenblick eine Reihe

$$p = p_0, p_1, \ldots, p_n = q$$

von Elementen von $\mathfrak{P}$, in der

$$(Ap_0, Ap_1) \neq 0, \ldots, (Ap_{n-1}, Ap_n) \neq 0.$$

Nach einem in § 3, **3** angeführten Hilfssatz über stetige lineare Funktionen gibt es zu jedem $y \in \mathfrak{R}$ ein z in dem vom Definitionsbereich von A erzeugten Unterraum derart, daß

$$(Ax, y) = (x, z)$$

ist für alle x des Definitionsbereichs von $\mathfrak{S}$. Ist $p \in \mathfrak{P}$ und setzt man $y = Ap$, so gibt es nach § 2, **3** zu dem zugehörigen z höchstens abzählbar viele $p_1 \in \mathfrak{P}$ mit $(p_1, z) \neq 0$, d. h. höchstens abzählbar viele $p_1 \in \mathfrak{P}$ mit $(Ap, Ap_1) \neq 0$. Zu jedem p_1 gibt es aus demselben Grunde höchstens abzählbar viele p_2 mit $(Ap_1, Ap_2) \neq 0$; darum kann man p auch nur mit höchstens abzählbar vielen q durch eine Kette von der Länge 2 verbinden. Analog kann man p nur mit höchstens abzählbar vielen $q \in \mathfrak{P}$ durch eine Kette von der Länge n verbinden, also kann man p überhaupt nur mit höchstens abzählbar vielen $q \in \mathfrak{P}$ durch eine Kette verbinden. Die Verbindbarkeit zweier Elemente von $\mathfrak{P}$ durch eine Kette ist nun offenbar eine Äquivalenzrelation, die eine Klasseneinteilung von $\mathfrak{P}$ liefert. In

dieser muß offensichtlich für p und q aus verschiedenen Klassen stets $Ap \perp Aq$ gelten, sonst wären ja p und q durch eine Kette von der Länge 1 verbindbar. Und daß die so entstehenden Klassen nie überabzählbar sind, wurde eben gezeigt.

Dieselbe Schlußweise liefert noch etwas mehr: Sind $A_1, A_2, \ldots$ höchstens abzählbar viele stetige Operatoren, deren Definitionsbereiche alle $\mathfrak{P}$ enthalten, so kann man $\mathfrak{P}$ auch in höchstens abzählbare Klassen so zerlegen, daß, wenn p und q in verschiedenen Klassen liegen, sogar

$$A_m p \perp A_n q$$

für alle m und alle n. Es ist wohl nicht nötig, das im einzelnen auseinanderzusetzen.

2. Wir ziehen eine erste Folgerung.

Die Linearmannigfaltigkeit $\mathfrak{S}$ sei durch den stetigen Operator A eineindeutig auf die Linearmannigfaltigkeit $\mathfrak{L}$ abgebildet. Ist dann $\mathfrak{P}$ ein Orthonormalsystem in $\mathfrak{S}$, so ist die Dimension von $\mathfrak{L}$ nicht kleiner als die Mächtigkeit von $\mathfrak{P}$.

Beweis. Wir teilen $\mathfrak{P}$ in die Klassen $\mathfrak{P}_\nu$ aus § 6, **1** ein. $\mathfrak{S}_\nu$ seien die von den einzelnen Klassen $\mathfrak{P}_\nu$ erzeugten Linearmannigfaltigkeiten (ν durchläuft, wie immer, eine beliebige Menge von Indizes). Weil $\mathfrak{P}_\nu$ Grundmenge in $\mathfrak{S}_\nu$ ist, ist $A\mathfrak{P}_\nu$ Grundmenge in $A\mathfrak{S}_\nu$, folglich ist $A\mathfrak{S}_\nu$ separabel. Nach § 5, **3** folgt (weil auch $\mathfrak{S}_\nu$ separabel ist)

$$\mathrm{Dim}\ \mathfrak{S}_\nu = \mathrm{Dim}\ A\mathfrak{S}_\nu .$$

Nach Konstruktion der Klasseneinteilung sind aber verschiedene $A\mathfrak{P}_\nu$ orthogonal, darum sind auch verschiedene $A\mathfrak{S}_\nu$ orthogonal. Ist $\mathfrak{L}'$ die von allen $A\mathfrak{S}_\nu$ zusammen erzeugte Linearmannigfaltigkeit, so ist $\mathfrak{L}' \subseteq \mathfrak{L}$ und nach § 5, **5**

$$\sum_\nu \mathrm{Dim}\ A\mathfrak{S}_\nu = \mathrm{Dim}\ \mathfrak{L}' .$$

Ist noch $\mathfrak{d}_\nu$ die Mächtigkeit von $\mathfrak{P}_\nu$ und $\mathfrak{d}$ die von $\mathfrak{P}$, so ist nach § 5, **6**

$$\mathfrak{d}_\nu = \mathrm{Dim}\ \mathfrak{S}_\nu ,$$

also

$$\mathfrak{d} = \sum_\nu \mathfrak{d}_\nu = \sum_\nu \mathrm{Dim}\ \mathfrak{S}_\nu = \sum_\nu \mathrm{Dim}\ A\mathfrak{S}_\nu = \mathrm{Dim}\ \mathfrak{L}' \subseteq \mathrm{Dim}\ \mathfrak{L}.$$

Ist insbesondere die Mächtigkeit von $\mathfrak{P}$ gleich Dim $\mathfrak{S}$ (ist z. B. $\mathfrak{P}$ in $\mathfrak{S}$ vollständig), so kann man aus § 5, **3** und dem eben Bewiesenen sofort schließen

$$\mathrm{Dim}\ \mathfrak{S} = \mathrm{Dim}\ \mathfrak{L}.$$

Weil es in Unterräumen stets vollständige Orthonormalsysteme gibt, folgt:

Alle eineindeutigen stetigen linearen Bilder eines Unterraums haben die gleiche Dimension wie der Unterraum.

Dies letztere Ergebnis hätten wir auch auf anderem Wege erhalten können: Nach dem auch in § 6, **1** benutzten Hilfssatz (den man aber dort leicht eliminieren kann) gibt es unter der Voraussetzung, daß $\mathfrak{S}$ Unterraum ist, zu jedem $y \in \mathfrak{S}$ genau ein $z = Hy \in \mathfrak{S}$ mit

$$(Ax, Ay) = (x, Hy) .$$

H ist, als Operator in $\mathfrak{S}$ angesehen, beschränkt und hermitesch. Ordnet man jedem $f \neq 0$ aus $\mathfrak{S}$ als $\mathfrak{M}(f)$ die aus $f, Hf, H^2f, \ldots$ bestehende Menge zu, so sind die Voraussetzungen von § 2, **5** erfüllt; es gibt also Elemente $f_\nu \neq 0$ in $\mathfrak{S}$ so, daß die $\mathfrak{S}_\nu = \mathfrak{M}(f_\nu)$ paarweise orthogonal sind und zusammen den Unterraum $\mathfrak{S}$ erzeugen. Aus $H\mathfrak{S}_\nu \subseteq \mathfrak{S}_\nu$ folgt $(Ax, Ay) = (Hx, y) = 0$, sowie $x \in \mathfrak{S}_\nu$, $y \in \mathfrak{S}_\mu$, $\nu \neq \mu$. Die $\mathfrak{S}_\nu$ und die $A\mathfrak{S}_\nu$ sind separabel, und auch die $A\mathfrak{S}_\nu$ bilden zusammen eine Grundmenge in $\mathfrak{L}$; daraus folgt

$$\mathrm{Dim}\ \mathfrak{S} = \sum_\nu \mathrm{Dim}\ \mathfrak{S}_\nu = \sum_\nu \mathrm{Dim}\ A\mathfrak{S}_\nu = \mathrm{Dim}\ \mathfrak{L} .$$

Der hier skizzierte Weg führt mit trivialer Abänderung auch zu den gleich abzuleitenden Sätzen über abgeschlossene Operatoren.

3. *A sei ein abgeschlossener Operator, $\mathfrak{D}$ sein Definitionsbereich, $\mathfrak{L}$ sein Wertebereich. A^{-1} existiere, d. h. A vermittle eine eineindeutige lineare Beziehung zwischen $\mathfrak{D}$ und $\mathfrak{L}$. Dann ist*

$$\operatorname{Dim}\mathfrak{D} = \operatorname{Dim}\mathfrak{L}.$$

Beweis. Der in § 3, **4** eingeführte Operator F ist als Projektor stetig und führt $\mathfrak{B}_A$ eineindeutig in $\{\mathfrak{D}, 0\}$ (die Menge der $\{x, 0\}$, $x \in \mathfrak{D}$) über. Genau so ist $\overline{E} - F$ ein stetiger Operator, der $\mathfrak{B}_A$ eineindeutig in $\{0, \mathfrak{L}\}$ überführt (eineindeutig wegen der Existenz von A^{-1}). Weil nach Voraussetzung $\mathfrak{B}_A$ Unterraum ist und weil man trivialerweise $\mathfrak{D}$ und $\mathfrak{L}$ isometrisch auf $\{\mathfrak{D}, 0\}$ bzw. $\{0, \mathfrak{L}\}$ abbilden kann, ist

$$\operatorname{Dim}\mathfrak{D} = \operatorname{Dim}\{\mathfrak{D}, 0\} = \operatorname{Dim}\mathfrak{B}_A = \operatorname{Dim}\{0, \mathfrak{L}\} = \operatorname{Dim}\mathfrak{L}.$$

A sei ein beliebiger abgeschlossener Operator des Raumes $\mathfrak{R}$. Dann gibt es paarweise orthogonale separable Unterräume von $\mathfrak{R}$, die A reduzieren (§ 4, **2**) *und die zusammen den Unterraum $\mathfrak{R}$ erzeugen.*

Beweis. $\mathfrak{P}$ sei ein vollständiges Orthonormalsystem in $\mathfrak{B}_A$. Nach dem Zusatz zu § 6, **1** gibt es zu den beiden stetigen Operatoren, die den $\{x, Ax\} \in \mathfrak{B}_A$ die Elemente x bzw. Ax von $\mathfrak{R}$ zuordnen, eine Einteilung von $\mathfrak{P}$ in höchstens abzählbare Klassen derart, daß, wenn $\{x, Ax\} \in \mathfrak{P}$ und $\{y, Ay\} \in \mathfrak{P}$ in verschiedenen Klassen sind, $x \perp y$ und $Ax \perp y$ und $x \perp Ay$ und $Ax \perp Ay$ gilt. Sind $\mathfrak{S}_\nu$ die von den verschiedenen Klassen von $\mathfrak{P}$ in $\mathfrak{B}_A$ erzeugten Unterräume, so gilt natürlich $x \perp y$, $Ax \perp y$, $x \perp Ay$, $Ax \perp Ay$ auch schon, wenn $\{x, Ax\}$ und $\{y, Ay\}$ in verschiedenen $\mathfrak{S}_\nu$ sind. Wir setzen nun

$$\mathfrak{S}'_\nu = \mathfrak{B}_A \ominus \mathfrak{S}_\nu$$

und definieren $\mathfrak{D}_\nu$, $\mathfrak{L}_\nu$, $\mathfrak{D}'_\nu$ und $\mathfrak{L}'_\nu$ durch

$$\{\mathfrak{D}_\nu, 0\} = F\mathfrak{S}_\nu, \qquad \{0, \mathfrak{L}_\nu\} = (\overline{E} - F)\mathfrak{S}_\nu,$$
$$\{\mathfrak{D}'_\nu, 0\} = F\mathfrak{S}'_\nu, \qquad \{0, \mathfrak{L}'_\nu\} = (\overline{E} - F)\mathfrak{S}'_\nu.$$

Aus

$$\mathfrak{B}_A = \mathfrak{S}_\nu \oplus \mathfrak{S}'_\nu$$

folgt dann

$$\mathfrak{D} = \mathfrak{D}_\nu \dotplus \mathfrak{D}'_\nu,$$

und es ist, wenn $\mathfrak{R}_\nu$ der von $\mathfrak{D}_\nu$ und $\mathfrak{L}_\nu$ zusammen erzeugte Unterraum ist,

$$\mathfrak{D}_\nu \leqq \mathfrak{R}_\nu, \qquad A\mathfrak{D}_\nu = \mathfrak{L}_\nu \leqq \mathfrak{R}_\nu,$$
$$\mathfrak{D}'_\nu \perp \mathfrak{R}_\nu, \qquad A\mathfrak{D}'_\nu = \mathfrak{L}'_\nu \perp \mathfrak{R}_\nu.$$

Nach § 4, **2** reduzieren demnach alle $\mathfrak{R}_\nu$ den abgeschlossenen Operator A. Mit den $\mathfrak{S}_\nu$ sind die $\mathfrak{D}_\nu$ und die $\mathfrak{L}_\nu$ und darum auch die $\mathfrak{R}_\nu$ separabel. Der von allen $\mathfrak{R}_\nu$ erzeugte Unterraum enthält aber Definitions- und Wertebereich von A. Sein orthogonales Komplement darf man also in beliebiger Weise in paarweise orthogonale separable (z. B. eindimensionale) Unterräume zerlegen, diese werden A trivialerweise auch reduzieren.

Aus dem damit bewiesenen Satz folgt, daß es irreduzible abgeschlossene Operatoren nur in separablen Räumen gibt.

In den separablen Linearmannigfaltigkeiten $\mathfrak{D}_\nu$ des obigen Beweises liefert uns das E. Schmidtsche Orthogonalisierungsverfahren vollständige Orthonormalsysteme. Wählt man in jedem $\mathfrak{D}_\nu$ eins aus und setzt man all diese Systeme zusammen, so erhält man in $\mathfrak{D}$ ein vollständiges Orthonormalsystem.

Dies Ergebnis, daß der Definitionsbereich jedes abgeschlossenen Operators ein vollständiges Orthonormalsystem enthält, legt die Frage nahe, ob es überhaupt Linearmannigfaltigkeiten gibt, in denen kein vollständiges Orthonormalsystem existiert. Diese Frage hat Wecken im bejahenden Sinne beantwortet [24]). Der Grundgedanke seiner Kon-

[24]) Rellich [2] S. 6, 7f.

struktion ist folgender: Man kann eine linear unabhängige Teilmenge eines separablen Hilbertschen Raums $\mathfrak{H}$ mit der Mächtigkeit des Kontinuums explizit angeben. Ihre Elemente f ordne man eineindeutig den Elementen p eines vollständigen Orthonormalsystems in einem Raum $\mathfrak{C}$, dessen Dimension gleich der Mächtigkeit des Kontinuums ist, zu. Nun denke man sich $\mathfrak{H}$ und $\mathfrak{C}$ senkrecht zueinander in einen großen Raum eingebettet und bilde in ihm die von den Summen $f + p$ einander zugeordneter f und p erzeugte Linearmannigfaltigkeit $\mathfrak{L}$. Diese erzeugt mit $\mathfrak{H}$ zusammen den Unterraum $\mathfrak{H} \oplus \mathfrak{C}$ und ist deshalb nicht separabel, trotzdem bildet der zu $\mathfrak{H}$ gehörige Projektor $\mathfrak{L}$ eineindeutig auf eine in $\mathfrak{H}$ enthaltene Linearmannigfaltigkeit, deren Dimension also höchstens $\mathfrak{a}$ ist, ab. Enthielte $\mathfrak{L}$ ein vollständiges Orthonormalsystem, so widerspräche das dem in § 6, 2 Festgestellten.

4. *Sind $\mathfrak{S}$ und $\mathfrak{T}$ Unterräume, $\mathfrak{D}$ ihr Durchschnitt und $\mathfrak{V}$ der von $\mathfrak{S}$ und $\mathfrak{T}$ erzeugte Unterraum, so ist*

$$\mathrm{Dim}(\mathfrak{T} \ominus \mathfrak{D}) = \mathrm{Dim}(\mathfrak{V} \ominus \mathfrak{S}).$$

Beweis. Es sei P der zu $\mathfrak{V} \ominus \mathfrak{S}$ gehörige Projektor,

$$P(\mathfrak{T} \ominus \mathfrak{D}) = \mathfrak{L}.$$

P ist jedenfalls ein Operator, der $\mathfrak{T} \ominus \mathfrak{D}$ stetig in $\mathfrak{L}$ transformiert. Diese Transformation ist eineindeutig, denn P führt Elemente von $\mathfrak{T} \ominus \mathfrak{D} \leqq \mathfrak{V}$ nur dann in 0 über, wenn sie in $\mathfrak{S}$ liegen, also in $\mathfrak{T} \cap \mathfrak{S} = \mathfrak{D}$, also in $(\mathfrak{T} \ominus \mathfrak{D}) \cap \mathfrak{D} = 0$. Daher (§ 6, 2)

$$\mathrm{Dim}\,(\mathfrak{T} \ominus \mathfrak{D}) = \mathrm{Dim}\,\mathfrak{L}.$$

$\mathfrak{S}$ und $\mathfrak{T} \ominus \mathfrak{D}$ sind zusammen Grundmenge in $\mathfrak{V}$, darum sind $P\mathfrak{S} = 0$ und $P(\mathfrak{T} \ominus \mathfrak{D}) = \mathfrak{L}$ zusammen Grundmenge in $P\mathfrak{V} = \mathfrak{V} \ominus \mathfrak{S}$, d. h. $\mathfrak{L}$ ist in $\mathfrak{V} \ominus \mathfrak{S}$ dicht, daher (§ 5, 4)

$$\mathrm{Dim}\,\mathfrak{L} = \mathrm{Dim}\,(\mathfrak{V} \ominus \mathfrak{S}).$$

Hiermit beweist man leicht

$$\mathrm{Dim}\,\mathfrak{S} + \mathrm{Dim}\,\mathfrak{T} = \mathrm{Dim}\,\mathfrak{V} + \mathrm{Dim}\,\mathfrak{D},$$

nämlich so:

$$\begin{aligned}\mathrm{Dim}\,\mathfrak{S} + \mathrm{Dim}\,\mathfrak{T} &= \mathrm{Dim}\,\mathfrak{S} + \mathrm{Dim}\,(\mathfrak{T} \ominus \mathfrak{D}) + \mathrm{Dim}\,\mathfrak{D} \\ &= \mathrm{Dim}\,\mathfrak{S} + \mathrm{Dim}\,(\mathfrak{V} \ominus \mathfrak{S}) + \mathrm{Dim}\,\mathfrak{D} \\ &= \mathrm{Dim}\,\mathfrak{V} + \mathrm{Dim}\,\mathfrak{D}.\end{aligned}$$

Aber es folgt noch mehr, nämlich:

$\mathfrak{R}_\nu$ sei eine wohlgeordnete Menge von Unterräumen: ν durchlaufe die Ordnungszahlen $0 \leqq \nu < \varrho$, wo ϱ eine passende Ordnungszahl ist. Für $\tau \leqq \varrho$ sei $\mathfrak{V}_\tau$ der von den $\mathfrak{R}_\nu$ mit $\nu < \tau$ erzeugte Unterraum, $\mathfrak{V}_0 = 0$, und für $\nu < \varrho$ habe $\mathfrak{R}_\nu$ nur 0 mit $\mathfrak{V}_\nu$ gemein. Dann ist

$$\mathrm{Dim}\,\mathfrak{V}_\varrho = \sum_{\nu<\varrho} \mathrm{Dim}\,\mathfrak{R}_\nu.$$

Beweis. Es sei für $\nu < \varrho$:

$$\mathfrak{S}_\nu = \mathfrak{V}_{\nu+1} \ominus \mathfrak{V}_\nu.$$

Dann ist, wie soeben festgestellt,

$$\mathrm{Dim}\,\mathfrak{R}_\nu = \mathrm{Dim}\,\mathfrak{S}_\nu \qquad (\nu < \varrho).$$

Die $\mathfrak{S}_\nu$ sind nun paarweise orthogonale Unterräume von $\mathfrak{V}_\varrho$. $\mathfrak{U}_\tau$ sei $(\tau \leqq \varrho)$ der von den $\mathfrak{S}_\nu$ mit $\nu < \tau$ erzeugte Unterraum, $\mathfrak{U}_0 = 0$. Aus

$$\mathfrak{S}_\nu \leqq \mathfrak{V}_{\nu+1} \leqq \mathfrak{V}_\tau \qquad (\nu < \tau)$$

folgt $\mathfrak{U}_\tau \leqq \mathfrak{V}_\tau$. Es gilt aber sogar

$$\mathfrak{U}_\tau = \mathfrak{V}_\tau.$$

Beweis durch transfinite Induktion: $\tau = 0$ klar. Sei schon $\mathfrak{U}_\nu = \mathfrak{V}_\nu$ für alle $\nu < \tau$. Dann ist für $\nu < \tau$ sowohl $\mathfrak{V}_\nu (= \mathfrak{U}_\nu)$ wie $\mathfrak{V}_{\nu+1} \ominus \mathfrak{V}_\nu (= \mathfrak{S}_\nu)$, mithin auch

$$\mathfrak{R}_\nu \leqq \mathfrak{V}_{\nu+1} = \mathfrak{V}_\nu \oplus (\mathfrak{V}_{\nu+1} \ominus \mathfrak{V}_\nu)$$

in $\mathfrak{U}_\tau$ enthalten, $\mathfrak{V}_\tau \leqq \mathfrak{U}_\tau$; weil $\mathfrak{U}_\tau \leqq \mathfrak{V}_\tau$ schon bewiesen ist, ist wirklich $\mathfrak{U}_\tau = \mathfrak{V}_\tau$. Insbesondere ist $\mathfrak{U}_\varrho = \mathfrak{V}_\varrho$. Da aber nach § 5, **5**

$$\operatorname{Dim} \mathfrak{U}_\varrho = \sum_{\nu<\varrho} \operatorname{Dim} \mathfrak{S}_\nu$$

ist, ist die Behauptung bewiesen.

5. Bei v. Neumann [25]) wird, wenn $\mathfrak{L}$ und $\mathfrak{M}$ Linearmannigfaltigkeiten mit $\mathfrak{L} \leqq \mathfrak{M}$ sind, eine Zahl Dim $\mathfrak{M}$ mod $\mathfrak{L}$ eingeführt, und zwar als Rang des Faktormoduls $\mathfrak{M}$ mod $\mathfrak{L}$, wenn dieser endlich ist; sonst wird Dim $\mathfrak{M}$ mod $\mathfrak{L} = \infty$ gesetzt. Dieser Begriff wird dort sogar noch verallgemeinert. Die obige Definition ist natürlich nur in separablen Räumen vernünftig. Wir werden jenen merkwürdigen Dimensionsbegriff zwar nicht brauchen, trotzdem soll hier wenigstens die Möglichkeit seiner Einführung in einer speziellen Klasse von Fällen, die aber doch für die Anwendungen ausreicht, bewiesen werden.

Dazu brauchen wir den Hilfssatz: Jeder abgeschlossene Operator B im Raum $\mathfrak{R}$, dessen Definitionsbereich ganz $\mathfrak{R}$ ist, ist beschränkt. Das beweist man vielleicht am einfachsten, indem man den Satz VI bei Hausdorff [1] S. 302f. auf die stetige lineare Abbildung

$$F\mathfrak{B}_B = \{\mathfrak{R}, 0\}$$

anwendet. Man kann den Hilfssatz aber auch wie Stone [1] S. 59ff. für selbstadjungiertes B beweisen und dann wie v. Neumann [3] S. 310 den allgemeinen Fall auf das schon Bewiesene zurückführen. Der Hilfssatz läßt sich übrigens in der allgemeineren Form aussprechen: *Sind B und C abgeschlossene Operatoren und enthält der Definitionsbereich von C den von B, so folgt aus* $\lim_{n\to\infty} x_n = x$ *und* $\lim_{n\to\infty} Bx_n = Bx$, *daß* $\lim_{n\to\infty} Cx_n = Cx$. Dies folgt aus dem oben angegebenen Spezialfall, indem man die Elemente von $\mathfrak{B}_B$ parallel zum Ordinatenraum so verschiebt, daß sie in $\mathfrak{B}_C$ fallen, und aus der Abgeschlossenheit dieser Transformation wie im folgenden Beweis auf ihre Stetigkeit schließt. In der Terminologie von Friedrichs [1] wird diese Überlegung noch einfacher.

Der Satz, der bewiesen werden soll, lautet:

$\mathfrak{L}$ und $\mathfrak{M}$ seien Linearmannigfaltigkeiten, $\mathfrak{L} \leqq \mathfrak{M}$, $\mathfrak{S}$ und $\mathfrak{T}$ seien Unterräume, $\mathfrak{S} \leqq \mathfrak{T}$. Der Operator A vermittle eine stetige und eineindeutige Abbildung seines Definitionsbereichs $\mathfrak{T}$ auf $\mathfrak{M}$, die $\mathfrak{S}$ in $\mathfrak{L}$ überführt. Dann ist Dim $(\mathfrak{T} \ominus \mathfrak{S})$ *nur von $\mathfrak{L}$ und $\mathfrak{M}$, nicht aber von $\mathfrak{S}$, $\mathfrak{T}$ und A abhängig.*

Beweis. Es seien auch $\bar{\mathfrak{S}}$ und $\bar{\mathfrak{T}}$ Unterräume, $\bar{\mathfrak{S}} \leqq \bar{\mathfrak{T}}$, und $\bar{A}$ vermittle eine eineindeutige und stetige Abbildung seines Definitionsbereichs $\bar{\mathfrak{T}}$ auf $\mathfrak{M}$, die $\bar{\mathfrak{S}}$ in $\mathfrak{L}$ überführt. Dann ist $\bar{A}^{-1}A$ ein Operator, der $\mathfrak{T}$ so auf $\bar{\mathfrak{T}}$ abbildet, daß $\mathfrak{S}$ in $\bar{\mathfrak{S}}$ übergeht. Aus $x_n \in \mathfrak{T}$, $x_n \to x$ und $\bar{A}^{-1}Ax_n \to y$ folgt $x \in \mathfrak{T}$, $Ax_n \to Ax$, $Ax_n = \bar{A}\bar{A}^{-1}Ax_n \to \bar{A}y$, $Ax = \bar{A}y$, $y = \bar{A}^{-1}Ax$. Also ist $\bar{A}^{-1}A$ abgeschlossen. Nach § 6, **3** gilt Dim $\mathfrak{T}$ = Dim $\bar{\mathfrak{T}}$, nach § 5, **6** gibt es einen isometrischen Operator U mit dem Definitionsbereich $\bar{\mathfrak{T}}$ und dem Wertebereich $\mathfrak{T}$. Nun ist $U\bar{A}^{-1}A$ ein abgeschlossener Operator in $\mathfrak{T}$ mit dem Definitionsbereich $\mathfrak{T}$, also nach dem Hilfssatz beschränkt. Das heißt: $\bar{A}^{-1}A$ ist stetig. Darum ist das Urbild $\mathfrak{U}$ des Unterraums $\bar{\mathfrak{T}} \ominus \bar{\mathfrak{S}}$ in $\mathfrak{T}$ ein Unterraum. Aus

$$\bar{\mathfrak{T}} = \bar{\mathfrak{S}} \oplus (\bar{\mathfrak{T}} \ominus \bar{\mathfrak{S}})$$

folgt

$$\mathfrak{T} = \mathfrak{S} \dotplus \mathfrak{U}.$$

Wegen § 6, **4** und § 6, **2** folgt

$$\operatorname{Dim} (\mathfrak{T} \ominus \mathfrak{S}) = \operatorname{Dim} \mathfrak{U} = \operatorname{Dim} (\bar{\mathfrak{T}} \ominus \bar{\mathfrak{S}}).$$

[25]) [1] S. 87.

Ob es aber zweckmäßig ist, die so als Funktion von $\mathfrak{L}$ und $\mathfrak{M}$ allein erkannte Kardinalzahl Dim $(\mathfrak{T} \ominus \mathfrak{S})$ mit Dim $\mathfrak{M}$ mod $\mathfrak{L}$ zu bezeichnen, bleibe dahingestellt.

§ 7. Der Spektralsatz.

1. Auch der Spektralsatz für selbstadjungierte Operatoren gehört wie die in § 3 zusammengestellten Tatsachen zu den in allen in dieser Arbeit betrachteten Räumen gültigen Sätzen. Aber der Umstand, daß (mit Ausnahme von Rellich [3] S. 5f.) in der Literatur kein Beweis vorkommt, der dies ganz klar zum Ausdruck kommen läßt [26]), zwingt uns doch zu näherer Betrachtung. Daß alle Beweise, die die Resolvente benutzen, nur im Hilbertschen Raum funktionieren, ist klar: Man kann eben $(A - \lambda E)^{-1}$ für komplexes λ nur bilden, wenn λE ein Operator ist. Man kann nun zwar aus der Gültigkeit des Spektralsatzes im Hilbertschen Raum seine Gültigkeit im reellen Hilbertschen Raum und dann auch im Wachsschen Raum erschließen, aber dieser Weg scheint mir nicht schön zu sein.

Erinnern wir uns lieber an Rieß [1], wo der Spektralsatz in einer in all' unseren Räumen gültigen Weise auf folgenden lokalen Zerlegungssatz zurückgeführt wird:

A sei selbstadjungiert. Dann gibt es einen Projektor P_- (er ist durch A eindeutig bestimmt und heiße der 0-Projektor von A) mit folgenden Eigenschaften:

1. *Aus $C \mathfrak{v} A$ folgt $C \mathfrak{v} P_-$.*
2. *$P_- \mathfrak{v} A$.*
3. *$A P_- \leqq 0$ [27]).*
4. *$A(E - P_-) \geqq 0$.*
5. *Aus $Ax = 0$ folgt $P_- x = 0$.*

Für beschränktes A läßt sich Rieß' Beweis wörtlich übertragen, einfacher steht der Beweis bei Wecken [1]. Für unbeschränktes A ist der Rießsche Beweis auf den Fall $\Sigma = K$ zugeschnitten. Man kann sich aber so helfen: Wie wir aus § 3, **4** wissen, ist, wenn A selbstadjungiert ist, $(A^2 + E)^{-1} = H$ ein beschränkter selbstadjungierter Operator [28]). Nicht allzu schwierige Rechnungen zeigen, daß $G = AH$ beschränkt und hermitesch ist, ferner daß $H \mathfrak{v} G$, $A = H^{-1} G$. Und daraus folgt durch ähnliche Rechnungen wie bei Rieß, daß der zu G gehörige 0-Projektor auch zu A als 0-Projektor gehört.

2. Es hätte nicht gelohnt, diesen Beweis in den Einzelheiten durchzuführen. Dafür wollen wir jetzt einen zweiten Beweis vollständig durchführen. Wir betrachten die Form (Ax, x) nicht als den x des Definitionsbereichs von A, sondern als den $\{x, Ax\}$ aus $\mathfrak{B}_A$ zugeordnet. Wegen

$$|(Ax, x)| \leqq \tfrac{1}{2} |\{x, Ax\}|^2$$

haben wir es mit einer beschränkten Form zu tun. Wenn wir aber $\mathfrak{B}_A$ orthogonal so zerlegt haben, daß (Ax, x) in einem Unterraum von $\mathfrak{B}_A$ negativ, im orthogonalen Komplement positiv semidefinit wird und der Unterraum sozusagen die Form (Ax, x) reduziert (von den unwesentlichen Bedingungen 1. und 5. einmal ganz abgesehen), haben wir durchaus keinen Grund zu der Annahme, dieser Tatbestand projizierte sich in den Abszissenraum. Man muß doch die Voraussetzung benutzen, daß nicht nur $A \leqq A^*$, sondern sogar $A = A^*$ ist, d. h.

$$\mathfrak{B}_A = \mathfrak{B}_{A^*} = \mathfrak{R}^2 \ominus V \mathfrak{B}_A .$$

---

[26]) Bei Friedrichs [1] § 5 ist allerdings der Spektralsatz für halbbeschränkte Operatoren allgemeingültig bewiesen und ein ähnlicher Beweis im allgemeinen Fall angekündigt.

[27]) Aus $P_- \mathfrak{v} A$ folgt $AP_- = P_- AP_- \leqq (P_- AP_-)^* = (AP_-)^* \leqq (P_- A)^* = AP_-$, darum ist AP_- selbstadjungiert.

[28]) Dasselbe folgt nach einer Bemerkung von F. J. Wecken durch Anwenden der Sätze Friedrichs' ([1]) auf die Form $(x, y) + (Ax, Ay)$.

Diese Voraussetzung besagt genau: Jedes Element $\{x, y\}$ von $\mathfrak{R}^2$ läßt sich in der Form

$$\{x, y\} = \{z, Az\} + \{A\zeta, -\zeta\}$$

darstellen (z, ζ im Definitionsbereich von A), und

$$\{z, Az\} \perp \{A\zeta, -\zeta\}.$$

Wir werden daher nicht die Form (Az, z) in $\mathfrak{B}_A$ betrachten, sondern die Form $(Az, z) + (\zeta, A\zeta)$ in ganz $\mathfrak{R}^2$. Und zwar werden wir den hermiteschen Operator D, der diese Form erzeugt:

$$(D\{x, y\}, \{x, y\}) = (Az, z) + (\zeta, A\zeta),$$

explizit angeben.

3. A sei selbstadjungiert, und B sei der zum Unterraum $\mathfrak{B}_A$ von $\mathfrak{R}^2$ gehörende Projektor. F und V seien wie in § 3, **4** erklärt. V transformiert $F\mathfrak{R}^2$ und $B\mathfrak{R}^2$ in ihr orthogonales Komplement, daher

$$(1)\qquad \begin{aligned} VFV^{-1} &= \overline{E} - F & V(\overline{E} - F)V^{-1} &= F \\ VBV^{-1} &= \overline{E} - B & V(\overline{E} - B)V^{-1} &= B. \end{aligned}$$

Es werde definiert

$$(2)\qquad D = BFVB - (E - B)FV(E - B)\ ^{29}).$$

Wir formen diesen Ausdruck um. Aus (1) folgt

$$0 = -BVB$$

und

$$0 = (\overline{E} - B)\, V(\overline{E} - B).$$

Durch Addition der letzten drei Gleichungen folgt

$$D = -B(V - FV)B + (\overline{E} - \mathrm{B})\,(V - FV)\,(\overline{E} - B)$$

$$(3)\qquad D = (\overline{E} - B)\,(\overline{E} - F)\,V(\overline{E} - B) - B(\overline{E} - F)VB$$

$$(4)\qquad D = -BVFB + (\overline{E} - B)\,VF(\overline{E} - B),$$

letzteres nach (1). Ferner folgt durch Auflösen der Klammern in (2)

$$D = \quad BFV + FVB - FV$$

$$D = BV - BVF - FBV \quad \text{(nach (1))}$$

$$(5)\qquad D = (E - F)\,BV(E - F) - FBVF.$$

Aus (2) folgt $B \mathfrak{v} D$. Transformiert man (2) mit V, so entsteht bei Berücksichtigung von (1)

$$VDV^{-1} = (\overline{E} - B)\,(\overline{E} - F)\,V(\overline{E} - B) - B(\overline{E} - F)\,VB = D$$

nach (3); mithin $V \mathfrak{v} D$. Bildet man nach den Regeln aus § 3, **2** in (2) D^*, so entsteht wegen $F^* = F$, $B^* = B$, $V^* = -V$

$$D^* = -BVFB + (E - B)VF(E - B) = D$$

nach (4); mithin ist der beschränkte Operator D hermitesch. Schließlich folgt aus (5) $F \mathfrak{v} D$.

Nach dem für beschränkte hermitesche Operatoren schon bewiesenen Zerlegungssatz gibt es zu dem beschränkten hermiteschen D einen 0-Projektor, der wie D (nach 1.) mit F und V vertauschbar sein muß und darum nach § 4, **3** in der Form $\overline{P_-}$ geschrieben werden kann. Mit $\overline{P_-}$ ist natürlich auch P_- Projektor. Wir behaupten, P_- sei der zu A gehörende 0-Projektor.

---

[29]) Es ist $D = \overline{A(A^2 + E)^{-1}}$. Dies liefert einen Zusammenhang mit dem vorhin gegebenen Beweis. Vgl. § 14, **4**.

Beweis. 1. Es gelte $C \mathfrak{v} A$. Dann gilt nach § 4, **1** $C^* \mathfrak{v} A^* = A$, nach § 4, **3** wird $\mathfrak{B}_A$ von $\overline{C}$ und $\overline{C^*} = \overline{C}^*$ in sich übergeführt, nach dem Zusatz von § 4, **2** folgt $\overline{C} \mathfrak{v} B$.

Nach § 4, **3** gilt außerdem $\overline{C} \mathfrak{v} F$ und $\overline{C} \mathfrak{v} V$, mithin

$$\overline{C} \mathfrak{v} BFVB - (\overline{E} - B)\, FV(\overline{E} - B) = D,$$
$$\overline{C} \mathfrak{v} \overline{P_-},$$
$$C \mathfrak{v} P_-.$$

2. Aus dem oben festgestellten $B \mathfrak{v} D$ folgt

$$B \mathfrak{v} \overline{P_-},$$
$$B\overline{P_-}B = \overline{P_-}B.$$

$\overline{P_-}$ führt demnach $\mathfrak{B}_A$ in sich über, nach § 4, **3** folgt

$$P_- \mathfrak{v} A\,.$$

3. $$\begin{aligned}(AP_-z, z) &= (\{AP_-z, 0\}, \{P_-z, AP_-z\}) \\ &= (FVB\overline{P_-}\{P_-z, AP_-z\}, \{P_-z, AP_-z\}) \\ &= (D\overline{P_-}\{P_-z, AP_-z\}, \{P_-z, AP_-z\}) \leqq 0.\end{aligned}$$

4. Entsprechend folgt $(A(E - P_-)z, z) \geqq 0$.

5. Aus $Az = 0$ folgt

$$D\{z, 0\} = BFV\{z, 0\} = 0,$$
$$\overline{P_-}\{z, 0\} = 0,$$
$$P_-z = 0.$$

§ 8. Quaternionendarstellungen.

1. Nachdem wir uns im ersten Teil der Arbeit mit den Begriffen befaßt haben, die sich in mehr oder weniger zwangsläufiger Weise aus dem gewöhnlichen Hilbertschen Raum bei unseren beiden Verallgemeinerungen — beliebige Dimension und als Grundkörper beliebige Divisionsalgebra über dem Körper R — übertragen und nachdem wir außerdem die Theorie der Dimension in § 5 und § 6 entwickelt haben, wenden wir uns jetzt den Veränderungen zu, die die Zulassung des nichtkommutativen Quaternionenkörpers Q als Grundkörper hervorruft. Natürlicher Ausgangspunkt ist die schon in § 3, **1** festgestellte Tatsache, daß λx im Wachsschen Raum $\mathfrak{R} = \mathfrak{W}$ nur für $\lambda \in Z = R$ definiert ist.

Betrachten wir dagegen eine Darstellung der Elemente von $\mathfrak{W}$ durch Vektoren

$$x = \begin{pmatrix} \xi_1 \\ \xi_2 \\ \cdot \\ \cdot \end{pmatrix}$$

mit eventuell nichtabzählbar vielen Koordinaten ξ_ν, so erscheint diese Beschränkung zuerst durchaus unvernünftig. Wie sich die Raumverknüpfungen in den (schon in § 2, **3** implizit aufgestellten) Formeln

$$\begin{pmatrix} \xi_1 \\ \xi_2 \\ \cdot \\ \cdot \end{pmatrix} + \begin{pmatrix} \eta_1 \\ \eta_2 \\ \cdot \\ \cdot \end{pmatrix} = \begin{pmatrix} \xi_1 + \eta_1 \\ \xi_2 + \eta_2 \\ \cdot \\ \cdot \end{pmatrix}, \quad \begin{pmatrix} \xi_1 \\ \xi_2 \\ \cdot \\ \cdot \end{pmatrix} a = \begin{pmatrix} \xi_1 a \\ \xi_2 a \\ \cdot \\ \cdot \end{pmatrix}, \quad \left(\begin{pmatrix} \xi_1 \\ \xi_2 \\ \cdot \\ \cdot \end{pmatrix}, \begin{pmatrix} \eta_1 \\ \eta_2 \\ \cdot \\ \cdot \end{pmatrix} \right) = \sum_\nu \overline{\eta}_\nu \xi_\nu$$

ausdrücken, so wird man versuchen, ganz naiv zu definieren:

$$\lambda \begin{pmatrix} \xi_1 \\ \xi_2 \\ \cdot \\ \cdot \end{pmatrix} = \begin{pmatrix} \lambda\xi_1 \\ \lambda\xi_2 \\ \cdot \\ \cdot \end{pmatrix}.$$

Man sieht sofort: mit $\sum_\nu |\xi_\nu|^2$ ist $\sum_\nu |\lambda\xi_\nu|^2$ konvergent, die Definition führt also aus

dem Raum nicht heraus. Es gilt:

$$(1)\quad \begin{cases} \lambda(xa+yb) = (\lambda x)a + (\lambda y)b. \\ |\lambda x| = |\lambda|\,|x|. \\ (\lambda+\mu)x = \lambda x + \mu x. \\ (\lambda\mu)x = \lambda(\mu x). \\ (\lambda x, y) = (x, \bar{\lambda} y). \\ \lambda x = x\lambda \text{ für } \lambda \in R. \end{cases}$$

Bei näherem Zusehen erlebt man aber zwei Enttäuschungen: Erstens ist unsere Definition nicht unitär-invariant. λx hängt nicht nur von λ und x, sondern auch von dem speziellen Koordinatensystem, in dem wir x als $\begin{pmatrix}\xi_1\\ \xi_2\\ \vdots\end{pmatrix}$ darstellen, ab. Zweitens: Ist z. B. Dim $\mathfrak{W} = 2$, so ist

$$A\begin{pmatrix}\xi_1\\ \xi_2\end{pmatrix} = \begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix}\xi_1\\ \xi_2\end{pmatrix} \qquad (a_{ik} \in Q)$$

ein beschränkter Operator, der genau dann hermitesch ist, wenn

$$a_{ik} = \overline{a_{ki}};$$

diese Bedingung ist z. B. für die Matrix

$$(a_{ik}) = \begin{pmatrix}0 & i\\ -i & 0\end{pmatrix}$$

erfüllt, und trotzdem ist

$$\begin{pmatrix}0 & i\\ -i & 0\end{pmatrix}\begin{pmatrix}k\\ 1\end{pmatrix} = j\begin{pmatrix}k\\ 1\end{pmatrix}.$$

Die hermitesch symmetrische Matrix $\begin{pmatrix}0 & i\\ -i & 0\end{pmatrix}$ scheint also den nichtreellen Eigenwert j zu haben. Bringt man $\begin{pmatrix}0 & i\\ -i & 0\end{pmatrix}$ dagegen auf Hauptachsen, so erhält man

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},$$

was diese Eigenschaft nicht mehr hat. Dies Beispiel zeigt uns auch schon, daß sich zur Behandlung gewisser Aufgaben das in dem einen Koordinatensystem definierte λx besser eignet als das in dem anderen Koordinatensystem definierte. Wir werden das später noch bestätigt finden.

All dem tragen wir Rechnung, indem wir, aus den Gleichungen (1) nur das Unitärinvariante herausziehend, definieren:

2. *Eine Quaternionendarstellung ist eine Funktion, die jedem $\lambda \in Q$ einen beschränkten Operator T_λ so zuordnet, daß*

$$(2)\quad \begin{cases} T_\lambda + T_\mu = T_{\lambda+\mu}. \\ T_\lambda T_\mu = T_{\lambda\mu}. \\ T_\lambda^* = T_{\bar{\lambda}}. \\ T_\lambda = \lambda E \qquad \textit{für } \lambda \in R. \end{cases}$$

Den Erörterungen des § 8, **1** entnimmt man: $\mathfrak{P}$ sei ein vollständiges Orthonormalsystem in $\mathfrak{W}$, dann wird durch

$$T_\lambda x = T_\lambda \sum_{\mathfrak{P}} p(x,p) = \sum_{\mathfrak{P}} p\lambda(x,p)$$

jedem $\lambda \in Q$ ein beschränkter Operator T_λ so zugeordnet, daß die Funktion T_λ von λ eine Quaternionendarstellung ist. Natürlich ist T_λ durch

$$(3)\qquad T_\lambda p = p\lambda \qquad (p \in \mathfrak{P})$$

als beschränkter Operator schon eindeutig festgelegt. Wir gehen jetzt umgekehrt von einer beliebigen Quaternionendarstellung aus und werden u. a. zeigen, daß es stets zu ihr ein vollständiges Orthonormalsystem $\mathfrak{P}$ mit (3) gibt, daß also auf die angegebene Art schon jede Quaternionendarstellung entsteht.

T_λ sei also eine Quaternionendarstellung. Dann sei $\mathfrak{H}$ die Menge aller $f \in \mathfrak{W}$ mit

$$T_\lambda f = f\lambda \quad \text{für alle } \lambda \in Q. \tag{4}$$

$\mathfrak{H}$ ist dann offenbar ein abgeschlossener R-Rechtsmodul, d. h. $\mathfrak{H}$ enthält mit f und g auch $fa + gb$, wenn $a, b \in R$, und enthält mit f_n auch $\lim\limits_{n\to\infty} f_n$, wenn dieser vorhanden ist. Wir können aber noch mehr aussagen: aus $f \in \mathfrak{H}$, $g \in \mathfrak{H}$ folgt $(f, g) \in R$, denn wegen

$$(f, g)\lambda = (f\lambda, g) = (T_\lambda f, g) = (f, T_\lambda^* g) = (f, T_{\bar\lambda} g) = (f, g\bar\lambda) = \lambda(f, g)$$

ist (f, g) mit allen $\lambda \in Q$ vertauschbar. Auf Grund der Definition in § 2, **1** und § 2, **6** müssen wir $\mathfrak{H}$ einen Raum mit dem Grundkörper R, einen reellen Hilbertschen Raum nennen. Die von $\mathfrak{H}$ in $\mathfrak{W}$ erzeugte Linearmannigfaltigkeit (also wieder Q als Grundkörper!) ist nun $\mathfrak{W}$, denn ist $x \in \mathfrak{W}$ beliebig, so setze man

$$f(x) = x - T_i x i - T_j x j - T_k x k;$$

dann ist

$$T_i f(x) = T_i x + x i - T_k x j + T_j x k = f(x) i$$

und analog für j und k, also $T_\lambda f(x) = f(x)\lambda$ für alle $\lambda \in Q$, $f(x) \in \mathfrak{H}$ und

$$\begin{aligned} f(x) - f(xi)i - f(xj)j - f(xk)k &= x - T_i x i - T_j x j - T_k x k - (xi + T_i x - T_j x k + T_k x j) i \\ &\quad - (xj + T_i x k + T_j x - T_k x i) j - (xk - T_i x j + T_j x i + T_k x) k = 4x. \end{aligned}$$

Nach § 2, **3** gibt es ein in $\mathfrak{H}$ vollständiges Orthonormalsystem $\mathfrak{P}$. Dies ist natürlich, als Teilmenge von $\mathfrak{W}$ betrachtet, ein in $\mathfrak{W}$ vollständiges Orthonormalsystem. Und jedes $p \in \mathfrak{P}$ liegt in $\mathfrak{H}$, daraus folgt (3).

Wir haben soeben jeder Quaternionendarstellung T_λ einen reellen Hilbertschen Raum $\mathfrak{H}$ zugeordnet, der im Sinne von § 5, **1** Grundmenge in $\mathfrak{W}$ ist. Weil jedes $T_\lambda (\lambda \in Q)$ als beschränkter Operator durch die Werte, die es in der Grundmenge $\mathfrak{H}$ annimmt, vollständig festgelegt ist, diese aber durch (4) gegeben sind, ist jeder Raum $\mathfrak{H}$ höchstens einer Quaternionendarstellung zugeordnet. Wir wollen noch zeigen, daß jeder reelle Hilbertsche Raum $\mathfrak{H}$, der Grundmenge in $\mathfrak{W}$ ist, wirklich einer T_λ zugeordnet ist. Dazu wählen wir am einfachsten ein in $\mathfrak{H}$ vollständiges Orthonormalsystem $\mathfrak{P}$, das dann von selbst in $\mathfrak{W}$ vollständig ist, und erklären T_λ durch (3). Für $f \in \mathfrak{H}$ sind dann alle (f, p) $(p \in \mathfrak{P})$ reell, also

$$T_\lambda f = \sum_{\mathfrak{P}} p\lambda(f, p) = \sum_{\mathfrak{P}} p(f, p)\lambda = f\lambda$$

in Übereinstimmung mit (4). Für den T_λ zugeordneten reellen Hilbertschen Teilraum $\mathfrak{H}'$ gilt also $\mathfrak{H} \subseteqq \mathfrak{H}'$. Wäre nicht $\mathfrak{H} = \mathfrak{H}'$, so gäbe es ein $h' \perp \mathfrak{H}$, $h' \neq 0$ in $\mathfrak{H}'$, während doch $\mathfrak{H}' \leq \mathfrak{W} = \widetilde{\mathfrak{H}}$ ist.

3. In bezug auf die beschränkten Operatoren T, die in einer Quaternionendarstellung die Rolle des T_i spielen können, sagen die Beziehungen (2) folgendes aus:

$$T^2 = -E, \quad T^* = -T. \tag{5}$$

Beschränkte Operatoren mit diesen beiden Eigenschaften (5) wollen wir *Imaginäroperatoren* nennen. Sie sind unitär. Sie beherrschen alles Folgende. Zunächst soll für sie die der vorstehenden analoge Rechnung durchgeführt werden.

T sei ein Imaginäroperator, $\mathfrak{H}$ die Menge der $f \in \mathfrak{W}$ mit

$$Tf = fi.$$

Dann ist $\mathfrak{H}$ abgeschlossener K-Rechtsmodul: aus $f, g \in \mathfrak{H}$, $a, b \in K$ folgt $fa + gb \in \mathfrak{H}$,

und aus $f_n \in \mathfrak{H}$, $\lim f_n = f$ folgt $f \in \mathfrak{H}$. Ferner folgt aus $f, g \in \mathfrak{H}$ auch $(f, g) \in K$, denn wegen

$$(f, g)i = (fi, g) = (Tf, g) = (f, T^*g) = -(f, Tg) = -(f, gi) = i(f, g)$$

ist (f, g) mit i vertauschbar; K ist aber gerade der Körper der mit i vertauschbaren Quaternionen. $\mathfrak{H}$ ist also ein Hilbertscher Raum. Und die von $\mathfrak{H}$ in $\mathfrak{W}$ erzeugte Linearmannigfaltigkeit ist $\mathfrak{W}$, denn setzt man

$$f(x) = x - Txi \quad (x \in \mathfrak{W}),$$

so ist

$$Tf(x) = Tx + xi = f(x)i,$$

also $f(x) \in \mathfrak{H}$, und es ist

$$f(x) - f(xj)j = x - Txi - (xj + Txk)j = 2x.$$

Die Überlegung geht nun ganz analog § 8, 2 weiter und ergibt: *Man erhält Imaginäroperatoren und man erhält jeden Imaginäroperator, wenn man in $\mathfrak{W}$ ein vollständiges Orthonormalsystem $\mathfrak{P}$ wählt und T gleich dem (existierenden und eindeutig bestimmten) beschränkten Operator T mit*

$$Tp = pi \quad (p \in \mathfrak{P})$$

setzt. Die oben erklärte Zuordnung eines Hilbertschen Teilraums von $\mathfrak{W}$ zu jedem Imaginäroperator in $\mathfrak{W}$ ist eine eineindeutige Abbildung der Menge aller Imaginäroperatoren in $\mathfrak{W}$ auf die Menge aller der Hilbertschen Teilräume, die in $\mathfrak{W}$ Grundmengen sind.

4. *Zu jedem selbstadjungierten Operator A gibt es eine mit A vertauschbare Quaternionendarstellung T_λ.*

Beweis. Jedem $f \neq 0$ aus $\mathfrak{W}$ werde als $\mathfrak{M}(f)$ die Menge aller $P_\mu f$ $(\mu \in R)$ zugeordnet, wo P_μ die Spektralschar von A ist. Aus bekannten Sätzen der Spektraltheorie, die natürlich im Wachsschen Raum genau wie anderswo gelten, folgt, daß die Voraussetzungen von § 2, 5 erfüllt sind. Es gibt also eine Menge $\mathfrak{F}$ so, daß die $\mathfrak{M}(f)$ $(f \in \mathfrak{F})$ paarweise orthogonal sind und zusammen den Unterraum $\mathfrak{W}$ erzeugen. Weil alle $(P_\mu f, P_\nu g)$ $(\mu, \nu \in R; f, g \in \mathfrak{F})$ reell sind [30]), ist die abgeschlossene Hülle des von allen $P_\mu f$ $(\mu \in R, f \in \mathfrak{F})$ erzeugten R-Rechtsmoduls ein reeller Hilbertscher Teilraum $\mathfrak{H}$ von $\mathfrak{W}$, der offenbar in $\mathfrak{W}$ Grundmenge ist. Er ist im Sinne von § 8, 2 einer Quaternionendarstellung T_λ zugeordnet. Jedes P_μ führt die Menge aller $P_\mu f$ $(\mu \in R, f \in \mathfrak{F})$, also auch $\mathfrak{H}$ in einen Teil von sich über, daher ist

$$T_\lambda P_\mu x = P_\mu x \lambda = P_\mu T_\lambda x$$

für alle $x \in \mathfrak{H}$; weil aber $\mathfrak{H}$ in $\mathfrak{W}$ Grundmenge ist, gilt die Operatorengleichung

$$T_\lambda P_\mu = P_\mu T_\lambda$$

für alle $\mu \in R$, $\lambda \in Q$. Weil somit jedes T_λ mit allen P_μ vertauschbar ist, gilt $T_\lambda \mathfrak{v} A$.

In Wirklichkeit sind sogar alle $\widetilde{\mathfrak{M}(f)}$ separabel, das haben wir aber beim Beweis nicht benutzt. Ist A beschränkt, so hätte man einfacher für $\mathfrak{M}(f)$ die aus $f, Af, A^2f, \ldots$ bestehende Menge nehmen können.

Aus dem eben bewiesenen Satz folgt, daß jeder selbstadjungierte Operator mit einem gewissen Imaginäroperator vertauschbar ist.

Man rechnet leicht allgemein nach, daß ein beschränkter Operator A in einem durch ein vollständiges Orthonormalsystem gegebenen Koordinatensystem dann und nur dann eine reelle Matrix (Aq, p) hat, wenn A mit der durch (3) dem Orthonormalsystem zugeordneten Quaternionendarstellung vertauschbar ist. Aus unserem Satz folgt also:

Zu jedem beschränkten hermiteschen Operator A in $\mathfrak{W}$ gibt es mindestens ein vollständiges Orthonormalsystem $\mathfrak{P}$, für das die Matrix (Aq, p) reell ist. A hat also, wenn

[30]) Nämlich $(P_\mu f, P_\nu g) = 0$ für $f \neq g$, $= (P_\varrho f, P_\varrho f)$ für $f = g$, $\varrho = \mathrm{Min}(\mu, \nu)$.

Dim $\mathfrak{W} = n < \infty$ *ist, n reelle Eigenwerte* $\lambda_1, \ldots, \lambda_n$, *nämlich die Wurzeln der Gleichung*

$$|(Aq, p) - \lambda(q, p)| = 0 \quad (p \text{ Zeilenindex}, q \text{ Spaltenindex}).$$

Dasselbe hätte man natürlich auch mit weniger Aufwand beweisen können.

§ 9. Normalformen für Imaginäroperatoren.

1. Nicht nur im Wachsschen Raum, auch in den beiden Hilbertschen Räumen definieren wir: Ein Imaginäroperator ist ein beschränkter Operator T mit

$$T^2 = -E, \qquad T^* = -T,$$

der also von selbst unitär ist. Oder: Ein Imaginäroperator ist ein unitärer Operator T mit

$$T^2 = -E.$$

Aus der letzteren Fassung folgt: Der Unterraum $\mathfrak{U}$ reduziere den Operator T. Dann ist T dann und nur dann in $\mathfrak{R}$ Imaginäroperator, wenn T in $\mathfrak{U}$ und auch in $\mathfrak{R} \ominus \mathfrak{U}$ Imaginäroperator ist.

Wir wollen nun einige Normalformen aufstellen, denen man es sofort ansieht, daß sie Imaginäroperatoren liefern. Dann werden wir uns mit der Aufgabe beschäftigen, gegebene Imaginäroperatoren auf alle möglichen Arten in eine der Normalformen zu bringen oder doch paarweise orthogonale Unterräume zu konstruieren, die zusammen den ganzen Raum $\mathfrak{R}$ als Unterraum erzeugen und in deren jedem T auf eine der Normalformen gebracht werden kann.

2. $\mathfrak{R}$ habe die gerade oder unendliche Dimension

$$\operatorname{Dim} \mathfrak{R} = \mathfrak{d} = 2\mathfrak{p}.$$

Dann gibt es nach § 5, **6** mindestens einen Unterraum $\mathfrak{Z}$ von $\mathfrak{R}$ so, daß

$$\operatorname{Dim} \mathfrak{Z} = \operatorname{Dim}(\mathfrak{R} \ominus \mathfrak{Z}) = \mathfrak{p}.$$

Gleichfalls nach § 5, **6** gibt es einen isometrischen Operator U mit dem Definitionsbereich $\mathfrak{Z}$ und dem Wertebereich $\mathfrak{R} \ominus \mathfrak{Z}$. P sei der zu $\mathfrak{Z}$ gehörige Projektor. *Dann ist*

$$T = UP - U^{-1}(E - P)$$

ein Imaginäroperator.

Beweis. T ist überall definiert, weil man U ungehindert auf Elemente des Wertebereichs $\mathfrak{Z}$ von P und U^{-1} (vorhanden, weil U isometrisch ist!) auf Elemente des Wertebereichs $\mathfrak{R} \ominus \mathfrak{Z}$ von $E - P$ anwenden kann. Daß T beschränkt ist, ist trivial. Schreibt man

$$T = (E - P)UP - PU^{-1}(E - P),$$

so kann man

$$T^2 = -E, \quad (Tx, y) = -(x, Ty)$$

sofort nachrechnen.

$$T = UP - U^{-1}(E - P)$$

ist die *erste Normalform.* Weil in ihre Definition die Struktur des Grundkörpers nicht eingeht, ist sie die wichtigste (vgl. § 10, **2**). Ist T bekannt, so ist die Normalform durch $\mathfrak{Z}$ vollständig bestimmt: U ist einfach die Transformation, die T auf $\mathfrak{Z}$ ausübt. Ein gegebener Unterraum spielt dann und nur dann in einer passenden Darstellung von T in der ersten Normalform die Rolle des $\mathfrak{Z}$, wenn für ihn

$$T\mathfrak{Z} = \mathfrak{R} \ominus \mathfrak{Z}$$

gilt. Um also alle Darstellungen eines gegebenen Imaginäroperators T in der ersten Normalform aufzufinden, braucht man nur nach allen Unterräumen $\mathfrak{Z}$ mit

$$\mathfrak{Z} \oplus T\mathfrak{Z} = \mathfrak{R}$$

zu fragen.

Ein Musterbeispiel für einen Imaginäroperator in der ersten Normalform ist der Operator V aus § 3, **4**, wo man für $\mathfrak{Z}$ am einfachsten den Ordinatenraum $(\overline{E} - F)\mathfrak{R}^2$ nimmt. U ist dann durch

$$U\{0, z\} = \{z, 0\}$$

gegeben.

3. Die zweite Normalform nimmt auf die Struktur des Grundkörpers Σ Bezug. Ist ε ein Element von Σ mit $\varepsilon^2 = -1$, woraus $|\varepsilon| = 1$ folgt, und ist $\mathfrak{P}$ ein vollständiges Orthonormalsystem, so wird durch

$$Tp = p\varepsilon \qquad (p \in \mathfrak{P})$$

ein beschränkter Operator T bestimmt, der sich als Imaginäroperator herausstellt. Das ist die *zweite Normalform.*

Es kommt also zunächst einmal darauf an, für welche $\varepsilon \in \Sigma$ die Beziehung $\varepsilon^2 = -1$ gilt. In $\Sigma = R$ gibt es überhaupt kein solches ε, im reellen Hilbertschen Razum gibt es also keine zweite Normalform. In $\Sigma = K$ gibt es zwei solche ε, nämlich $\varepsilon = i$ und $\varepsilon = -i$. K ist aber kommutativ, daher kann man statt $Tp = p\varepsilon$ auch schreiben

$$Tp = \varepsilon p \quad (p \in \mathfrak{P})$$

oder

$$T = \pm iE.$$

Das sind also im Hilbertschen Raum die beiden Imaginäroperatoren der zweiten Normalform.

In $\Sigma = Q$ gibt es zu jedem ε mit $\varepsilon^2 = -1$ ein η mit

$$\varepsilon\eta = \eta i,$$

o. B. d. A. kann man sogar $|\eta| = 1$ annehmen [31]). $\mathfrak{P}\eta$, die Menge aller $p\eta$ $(p \in \mathfrak{P})$, ist dann auch ein vollständiges Orthonormalsystem, und aus

$$Tp = p\varepsilon$$

wird

$$T(p\eta) = (p\eta)i.$$

Im Wachsschen Raum dürfen wir uns daher o. B. d. A. auf $\varepsilon = i$ beschränken.

4. Wir wollen nun zuerst die Imaginäroperatoren im Hilbertschen Raum und im Wachsschen Raum auf die zweite Normalform bringen, um dann hiervon später zur ersten Normalform überzugehen.

T sei Imaginäroperator im Hilbertschen Raum $\mathfrak{H}$. Dann ist

$$P = \frac{E - iT}{2},$$

wie man sofort bestätigt, Projektor:

$$P^2 = \frac{E - 2iT - T^2}{4} = \frac{2E - 2iT}{4} = P,$$

$$P^* = \frac{E + iT^*}{2} = \frac{E - iT}{2} = P.$$

Ist $\mathfrak{U}$ der Unterraum der u mit $Pu = u$, $\mathfrak{V}$ der Unterraum der v mit $Pv = 0$, so ist $\mathfrak{H} = \mathfrak{U} \oplus \mathfrak{V}$, und $\mathfrak{U}$ ist die Menge der u mit $Tu = ui$, $\mathfrak{V}$ ist die Menge der v mit $Tv = -vi$, $\mathfrak{U}$ und $\mathfrak{V}$ reduzieren T. $\mathfrak{H}$ ist also direkte Summe zweier orthogonaler Unterräume, in deren jedem T die zweite Normalform hat. $\mathfrak{U}$ und $\mathfrak{V}$ sind offensichtlich durch T eindeutig bestimmt.

---

[31]) Man kann sogar noch $\eta^2 = -1$ annehmen: $\eta = \pm \frac{\varepsilon + i}{|\varepsilon + i|}$ für $\varepsilon \neq -i$, $\eta = aj + bk$ $(a, b \in R,$ $a^2 + b^2 = 1)$ für $\varepsilon = -i$.

Wir wissen aus § 8, **3**, daß man jeden Imaginäroperator im Wachsschen Raum in die zweite Normalform bringen kann.

5. Nun fragen wir nach denjenigen Unterräumen, in denen man einen gegebenen Imaginäroperator T in die erste Normalform bringen kann. Ist $\mathfrak{S}$ ein derartiger Unterraum, so soll also

$$\mathfrak{S} = \mathfrak{Z} \oplus T\mathfrak{Z}$$

mit passendem Unterraum $\mathfrak{Z}$ gelten. Insbesondere muß

$$T\mathfrak{Z} \perp \mathfrak{Z}$$

gelten. Ist aber dies erfüllt, so wird durch

$$\mathfrak{S} = \mathfrak{Z} \oplus T\mathfrak{Z}$$

ein Unterraum $\mathfrak{S}$ von $\mathfrak{R}$ definiert, in dem T die erste Normalform hat und der offenbar T reduziert. Wir können also die Fragestellung dahin abändern, daß wir nach allen Unterräumen $\mathfrak{Z}$ von $\mathfrak{R}$ fragen, für die $T\mathfrak{Z} \perp \mathfrak{Z}$ gilt.

T sei Imaginäroperator im reellen Hilbertschen Raum $\mathfrak{H}$. Dann kann man T in die erste Normalform bringen.

Beweis. Im reellen Hilbertschen Raum gilt identisch

$$(Tf, f) = (f, T^*f) = (f, -Tf) = -\overline{(Tf, f)} = -(Tf, f),$$

also

$$(Tf, f) = 0.$$

Man ordne jedem $f \neq 0$ aus $\mathfrak{H}$ als $\mathfrak{M}(f)$ die aus f und Tf bestehende Menge zu. Dann sind die Voraussetzungen von § 2, **5** erfüllt:

$$f \in \mathfrak{M}(f) < \widetilde{\mathfrak{M}(f)}$$

ist trivial, und aus $\mathfrak{M}(f) \perp g$ folgt

$$(f, g) = 0 \qquad (Tf, g) = 0$$
$$(f, Tg) = -(Tf, g) = 0, \qquad (Tf, Tg) = (f, g) = 0,$$
$$\mathfrak{M}(f) \perp \mathfrak{M}(g).$$

Darum gibt es Elemente f_ν in $\mathfrak{H}$ (wo ν irgendeine Menge von Indizes durchläuft) so, daß die $\mathfrak{M}(f_\nu)$ paarweise orthogonal sind und zusammen den Unterraum $\mathfrak{H}$ erzeugen. Wir können $|f_\nu| = 1$ annehmen. Dann ist auch $|Tf_\nu| = 1$ und $(Tf_\nu, f_\nu) = 0$. Die f_ν bilden daher mit den Tf_ν zusammen ein vollständiges Orthonormalsystem in $\mathfrak{H}$. Setzt man für $\mathfrak{Z}$ den von allen f_ν erzeugten Unterraum ein, so ist offenbar

$$\mathfrak{H} = \mathfrak{Z} \oplus T\mathfrak{Z}.$$

Die Unterräume von $\mathfrak{H}$, in denen man T auf die erste Normalform bringen kann, sind demnach alle Unterräume, die T überhaupt reduzieren. Als Nebenresultat stellt sich heraus, daß es in reellen Hilbertschen Räumen von ungerader Dimension keine Imaginäroperatoren gibt, weil dort die Gleichung

$$\mathrm{Dim}\,\mathfrak{H} = 2\,\mathrm{Dim}\,\mathfrak{Z}$$

unlösbar wird.

6. T sei ein Imaginäroperator im Hilbertschen Raum $\mathfrak{H}$, $\mathfrak{U}$ und $\mathfrak{V}$ die beiden in § 8, **4** eingeführten Unterräume, also

$$\mathfrak{H} = \mathfrak{U} \oplus \mathfrak{V}$$
$$Tu = ui \quad (u \in \mathfrak{U}), \qquad Tv = -vi \quad (v \in \mathfrak{V}).$$

Wir fragen nach den Unterräumen $\mathfrak{Z}$ mit $T\mathfrak{Z} \perp \mathfrak{Z}$. Ist uns solch ein $\mathfrak{Z}$ gegeben, so stellen wir gemäß $\mathfrak{H} = \mathfrak{U} \oplus \mathfrak{V}$ jedes $z \in \mathfrak{Z}$ eindeutig in der Form

$$z \in \mathfrak{Z}: \qquad z = u + v, \quad u \in \mathfrak{U}, \quad v \in \mathfrak{V}$$

dar. Nun ist $\mathfrak{U} \cap \mathfrak{Z} = 0$, denn für ein $u \in \mathfrak{U} \cap \mathfrak{Z}$ gilt zugleich $Tu = ui$ und $Tu \perp u$,

woraus $ui \perp u$, $u = 0$ folgt. Analog ist $\mathfrak{V} \cap \mathfrak{Z} = 0$. Daher gibt es zu jedem $u \in \mathfrak{U}$ höchstens ein $v \in \mathfrak{V}$ mit $u + v \in \mathfrak{Z}$, und zu jedem $v \in \mathfrak{V}$ gibt es höchstens ein $u \in \mathfrak{U}$ mit $u + v \in \mathfrak{Z}$. Durch

$$u + v \in \mathfrak{Z}$$

wird eine Teilmenge $\mathfrak{N}$ von $\mathfrak{V}$ eineindeutig und linear auf eine Teilmenge $\mathfrak{M}$ von $\mathfrak{U}$ abgebildet:

$$u = Sv, \qquad v = S^{-1}u.$$

$\mathfrak{N}$ ist einfach die Menge der $v \in \mathfrak{V}$, zu denen es ein $u(= Sv)$ in $\mathfrak{U}$ mit $u + v \in \mathfrak{Z}$ gibt, $\mathfrak{M} = S\mathfrak{N}$.

Der hierdurch definierte Operator S mit dem Definitionsbereich $\mathfrak{N} \leqq \mathfrak{V}$ und dem Wertebereich $\mathfrak{M} \leqq \mathfrak{U}$ ist nun isometrisch, und $\mathfrak{M}$ und $\mathfrak{N}$ sind Unterräume. Denn sobald $v \in \mathfrak{N}$ und $v' \in \mathfrak{N}$, d. h. $Sv + v \in \mathfrak{Z}$ und $Sv' + v' \in \mathfrak{Z}$ gilt, ist wegen $T\mathfrak{Z} \perp \mathfrak{Z}$

$$T(Sv + v) \perp Sv' + v', \qquad (Svi - vi, Sv' + v') = 0,$$

und wegen $S\mathfrak{N} = \mathfrak{M} \leqq \mathfrak{U} \perp \mathfrak{V} \geqq \mathfrak{N}$

$$(Sv, Sv') - (v, v') = 0,$$

womit schon gezeigt ist, daß S isometrisch ist. Es sei nun $v_n \in \mathfrak{V}$, $v_n \to v$. Dann ist auch

$$\lim_{m,n\to\infty} |Sv_m - Sv_n| = \lim_{m,n\to\infty} |v_m - v_n| = 0,$$

es konvergiert $Sv \to u$; aus

$$Sv_n + v_n \in \mathfrak{Z}$$

folgt, weil $\mathfrak{Z}$ Unterraum ist,

$$u + v \in \mathfrak{Z},$$

d. h. $Sv = u$, $v \in \mathfrak{N}$. Genau so beweist man die Abgeschlossenheit von $\mathfrak{M}$.

Zusammengefaßt: *Zu jedem Unterraum $\mathfrak{Z}$ mit $T\mathfrak{Z} \perp \mathfrak{Z}$ gibt es einen Unterraum $\mathfrak{M} \leqq \mathfrak{U}$, einen Unterraum $\mathfrak{N} \leqq \mathfrak{V}$ und einen isometrischen Operator S mit dem Definitionsbereich $\mathfrak{N}$ und dem Wertebereich $\mathfrak{M}$ so, daß $\mathfrak{Z}$ genau die Menge der $Sv + v (v \in \mathfrak{N})$, d. h. der Wertebereich von $E + S$, ist. Und ist*

$$\begin{aligned} \operatorname{Dim}\mathfrak{M} = \operatorname{Dim}\mathfrak{N} &= \mathfrak{p}, \\ \operatorname{Dim}\mathfrak{U} = \mathfrak{m}, \qquad & \operatorname{Dim}\mathfrak{V} = \mathfrak{n}, \\ \operatorname{Dim}(\mathfrak{U} \ominus \mathfrak{M}) = \mathfrak{m}', \qquad & \operatorname{Dim}(\mathfrak{V} \ominus \mathfrak{N}) = \mathfrak{n}', \end{aligned}$$

so ist

$$\mathfrak{m} = \mathfrak{p} + \mathfrak{m}', \qquad \mathfrak{n} = \mathfrak{p} + \mathfrak{n}'.$$

Dieser Tatbestand läßt sich umkehren. Sind nämlich Kardinalzahlen $\mathfrak{p}$, $\mathfrak{m}'$ und $\mathfrak{n}'$ so gegeben, daß

$$\mathfrak{p} + \mathfrak{m}' = \mathfrak{m} = \operatorname{Dim}\mathfrak{U}, \qquad \mathfrak{p} + \mathfrak{n}' = \mathfrak{n} = \operatorname{Dim}\mathfrak{V}$$

ist, dann gibt es Unterräume $\mathfrak{M} \leqq \mathfrak{U}$ und $\mathfrak{N} \leqq \mathfrak{V}$ mit

$$\begin{aligned} \operatorname{Dim}\mathfrak{M} = \mathfrak{p}, \qquad & \operatorname{Dim}\mathfrak{N} = \mathfrak{p}, \\ \operatorname{Dim}(\mathfrak{U} \ominus \mathfrak{M}) = \mathfrak{m}', \qquad & \operatorname{Dim}(\mathfrak{V} \ominus \mathfrak{N}) = \mathfrak{n}', \end{aligned}$$

und es gibt einen isometrischen Operator S mit dem Definitionsbereich $\mathfrak{N}$ und dem Wertebereich $\mathfrak{M}$. Erklärt man $\mathfrak{Z}$ als Wertebereich von $E + S$,

$$\mathfrak{Z} = (E + S)\mathfrak{N},$$

so folgt in bekannter Weise aus

$$|v + Sv|^2 = |v|^2 + |Sv|^2 = 2|v|^2$$

(wegen $Sv \perp v$), daß mit $\mathfrak{N}$ auch $\mathfrak{Z}$ abgeschlossen, also Unterraum ist. Und es ist

$$T(Sv + v) = (Sv - v)i,$$

$$(T(Sv + v), Sv' + v') = (Sv - v, Sv' + v')i = ((Sv, Sv') - (v, v'))\,i = 0,$$

also in der Tat

$$T\mathfrak{Z} \perp \mathfrak{Z}.$$

Wir können hinzufügen: Es ist

$$\mathfrak{Z} \oplus T\mathfrak{Z} = \mathfrak{M} \oplus \mathfrak{N},$$

denn $\mathfrak{Z}$ ist der Wertebereich von $E + S$ und $T\mathfrak{Z}$ der von $E - S$. Man kann schreiben

$$\mathfrak{H} = (\mathfrak{Z} \oplus T\mathfrak{Z}) \oplus (\mathfrak{U} \ominus \mathfrak{M}) \oplus (\mathfrak{V} \ominus \mathfrak{N}),$$

wo alle drei Summanden T reduzieren; T hat im ersten Summanden mit der Dimension $2\mathfrak{p}$ die erste Normalform, im zweiten und dritten Summanden mit den Dimensionen $\mathfrak{m}'$, $\mathfrak{n}'$ dagegen jeweils die zweite Normalform. Und zwischen $\mathfrak{p}$, $\mathfrak{m}'$ und $\mathfrak{n}'$ bestehen nur die Bedingungen

$$\mathfrak{m} = \mathfrak{p} + \mathfrak{m}', \qquad \mathfrak{n} = \mathfrak{p} + \mathfrak{n}',$$

sonst kann man sie beliebig vorschreiben.

7. T sei endlich ein Imaginäroperator im Wachsschen Raum $\mathfrak{W}$. Wir fragen nach den Unterräumen $\mathfrak{Z}$ mit

$$T\mathfrak{Z} \perp \mathfrak{Z}.$$

Ist uns solch ein $\mathfrak{Z}$ gegeben, so sei $\{p_\nu\}$, wo ν eine Menge von Indizes durchläuft, ein vollständiges Orthonormalsystem in $\mathfrak{Z}$. Wir definieren q_ν und q'_ν durch

$$\sqrt{2}\, q_\nu = p_\nu - Tp_\nu i, \qquad \sqrt{2}\, q'_\nu = -p_\nu j - Tp_\nu k.$$

Dann ist

$$Tq_\nu = q_\nu i, \; Tq'_\nu = q'_\nu i,$$

$$\sqrt{2}\, p_\nu = q_\nu + q'_\nu j, \; \sqrt{2}\, Tp_\nu = q_\nu i + q'_\nu k,$$

$$(q_\mu, q_\nu) = \tfrac{1}{2}(p_\mu - Tp_\mu i, \; p_\nu - Tp_\nu i) = (p_\mu, p_\nu) = \begin{cases} 1, & \mu = \nu \\ 0, & \mu \neq \nu, \end{cases}$$

$$(q'_\mu, q'_\nu) = \tfrac{1}{2}(p_\mu j + Tp_\mu k, p_\nu j + Tp_\nu k) = (p_\mu, p_\nu) = \begin{cases} 1, & \mu = \nu \\ 0, & \mu \neq \nu, \end{cases}$$

$$(q_\mu, q'_\nu) = -\tfrac{1}{2}(p_\mu - Tp_\mu i, p_\nu j + Tp_\nu k) = \tfrac{1}{2}(j(p_\mu, p_\nu) - k(p_\mu, p_\nu)i) = 0.$$

Das heißt: *Ist $\mathfrak{H}$ der aus § 8, 3 bekannte Hilbertsche Teilraum aller $f \in \mathfrak{W}$ mit $Tf = fi$, so sind die q_ν und die q'_ν zusammen ein Orthonormalsystem in $\mathfrak{H}$, das in $\mathfrak{W}$ den Unterraum $\mathfrak{Z} \oplus T\mathfrak{Z}$ erzeugt. Ist $\mathfrak{d}$ die Dimension von $\mathfrak{W}$, $\mathfrak{p}$ die von $\mathfrak{Z}$ und $\mathfrak{d}'$ die von $\mathfrak{W} \ominus (\mathfrak{Z} \oplus T\mathfrak{Z})$, so ist*

$$\mathfrak{d} = 2\,\mathfrak{p} + \mathfrak{d}'.$$

Dieser Tatbestand läßt sich umkehren. Seien nämlich die q_ν und die q'_ν, wo ν eine Indizesmenge von der Mächtigkeit $\mathfrak{p}$ durchläuft, zusammen ein Orthonormalsystem in $\mathfrak{H}$ [32]). Setzt man dann

$$\sqrt{2}\, p_\nu = q_\nu + q'_\nu j,$$

so ist

$$\sqrt{2}\, Tp_\nu = q_\nu i + q'_\nu k,$$

$$(p_\mu, p_\nu) = \frac{1}{2}(q_\mu + q'_\mu j, q_\nu + q'_\nu j) = \frac{(q_\mu, q_\nu) + (q'_\mu, q'_\nu)}{2} = \begin{cases} 1, & \mu = \nu \\ 0, & \mu \neq \nu, \end{cases}$$

$$(Tp_\mu, p_\nu) = \frac{1}{2}(q_\mu i + q'_\mu k, q_\nu + q'_\nu j) = \frac{(q_\mu, q_\nu)\, i - j(q'_\mu, q'_\nu)\, k}{2} = 0.$$

Das heißt: die p_ν sind ein Orthonormalsystem; ist $\mathfrak{Z}$ der davon erzeugte Unterraum, so $T\mathfrak{Z} \perp \mathfrak{Z}$.

[32]) Durch die Schreibweise deuten wir schon an, daß immer q_ν und q'_ν einander zugeordnet sind.

Sind ferner Kardinalzahlen $\mathfrak{p}$ und $\mathfrak{d}'$ gegeben, die nur der Bedingung

$$2\mathfrak{p} + \mathfrak{d}' = \mathfrak{d} = \operatorname{Dim} \mathfrak{W}$$

genügen, so gibt es nach § 5, **6** Elemente q_ν und q'_ν in $\mathfrak{H}$, wo ν eine Indizesmenge von der Mächtigkeit $\mathfrak{p}$ durchläuft, die zusammen ein Orthonormalsystem bilden, derart, daß die Dimension des orthogonalen Komplements in $\mathfrak{H}$ des von den q_ν und den q'_ν erzeugten Unterraums gerade gleich $\mathfrak{d}'$ wird. Konstruiert man $\mathfrak{Z}$ aus den q_ν und q'_ν wie eben angegeben, so ist $T\mathfrak{Z} \perp \mathfrak{Z}$, $\mathfrak{Z}$ hat die Dimension $\mathfrak{p}$, und $\mathfrak{W} \ominus (\mathfrak{Z} \oplus T\mathfrak{Z})$ ist das orthogonale Komplement des von den q_ν, q'_ν erzeugten Unterraums in $\mathfrak{W}$ und hat als solches die Dimension $\mathfrak{d}'$.

Wir können also die Unterräume $\mathfrak{Z}$ mit $T\mathfrak{Z} \perp \mathfrak{Z}$ durch die Orthonormalsysteme in $\mathfrak{H}$, die in zwei Klassen einander eineindeutig zugeordneter Elemente q_ν, q'_ν zerfallen, vollständig beschreiben. Und zwischen der Dimension $\mathfrak{p}$ von $\mathfrak{Z}$ und der Dimension $\mathfrak{d}'$ von $\mathfrak{W} \ominus (\mathfrak{Z} \oplus T\mathfrak{Z})$ besteht nur die eine Relation

$$(*) \qquad \mathfrak{d} = 2\mathfrak{p} + \mathfrak{d}'.$$

Jetzt lassen sich leicht die verschiedenen möglichen Fälle durchdiskutieren. Ist $\mathfrak{d} = 0$ oder $\mathfrak{d} = 1$, so kommt in (*) nur $\mathfrak{p} = 0$ in Frage, es ist notwendig $\mathfrak{Z} = 0$. Ist aber $\mathfrak{d} > 1$, so gibt es positive Zahlen $\mathfrak{p}$, für die (*) mit passendem $\mathfrak{d}'$ erfüllt ist. Ist $\mathfrak{d}$ gerade, so kann man durch passende Wahl von $\mathfrak{p}$ erreichen, daß $\mathfrak{d}' = 0$, man kann aber nicht $\mathfrak{d}' = 1$ erreichen; ist $\mathfrak{d}$ ungerade, so kann man wohl $\mathfrak{d}' = 1$, nicht aber $\mathfrak{d}' = 0$ durch richtige Wahl von $\mathfrak{p}$ erreichen. Ist $\mathfrak{d}$ schließlich unendlich, so kann man sowohl $\mathfrak{d}' = 0$ wie $\mathfrak{d}' = 1$ erreichen, indem man $\mathfrak{p} = \mathfrak{d}$ setzt.

Wir werden diese Ergebnisse im nächsten Abschnitt anwenden.

§ 10. Hermitesche abgeschlossene Operatoren.

1. Der Operator A heißt hermitesch, wenn A^* existiert und

$$A \leqq A^*$$

gilt, abgeschlossen, wenn $\mathfrak{B}_A$ abgeschlossen ist (A^* ist, wenn vorhanden, von selbst abgeschlossen), maximal, wenn er hermitesch und abgeschlossen ist, während keine echte Fortsetzung von A hermitesch und abgeschlossen ist, selbstadjungiert, wenn $A = A^*$, nurmaximal, wenn A maximal und nicht selbstadjungiert ist.

A sei ein fester hermitescher abgeschlossener Operator. Es sei

$$\mathfrak{L} = \mathfrak{B}_{A^*} \ominus \mathfrak{B}_A .$$

Nun ist nach § 3, **4**

$$\mathfrak{B}_{A^*} = \mathfrak{R}^2 \ominus V\mathfrak{B}_A .$$

Darum

$$\mathfrak{L} = (\mathfrak{R}^2 \ominus V\mathfrak{B}_A) \ominus \mathfrak{B}_A ,$$
$$\mathfrak{L} = \mathfrak{R}^2 \ominus (V\mathfrak{B}_A \oplus \mathfrak{B}_A) .$$

Weil V unitär ist, folgt

$$V\mathfrak{L} = V\mathfrak{R}^2 \ominus (V^2\mathfrak{B}_A \oplus V\mathfrak{B}_A) = \mathfrak{R}^2 \ominus (\mathfrak{B}_A \oplus V\mathfrak{B}_A) = \mathfrak{L} .$$

V führt also $\mathfrak{L}$ und auch das orthogonale Komplement von $\mathfrak{L}$ in $\mathfrak{R}^2$ in sich über, $\mathfrak{L}$ reduziert V. V kann daher auch als Operator in $\mathfrak{L}$ angesehen werden. Wie schon in § 9, **2** bemerkt, ist V Imaginäroperator. Wir werden bald die Ergebnisse des vorigen Abschnitts auf den Imaginäroperator V in $\mathfrak{L}$ anwenden.

Wegen $\mathfrak{L} \leqq \mathfrak{B}_{A^*}$ hat sicher jedes Element von $\mathfrak{L}$ die Form $\{z, A^*z\}$. Wir wollen die notwendige und hinreichende Bedingung dafür aufstellen, daß ein $\{z, A^*z\}$ in $\mathfrak{L}$ liegt. $\{z, A^*z\}$ liegt dann und nur dann in $\mathfrak{L}$, wenn

$$\{z, A^*z\} \perp \mathfrak{B}_A .$$

Weil V unitär ist, ist das gleichbedeutend mit

$$V\{z, A^*z\} \perp V\mathfrak{B}_A,$$
$$\{A^*z, -z\} \in \mathfrak{R}^2 \ominus V\mathfrak{B}_A = \mathfrak{B}_{A^*}.$$

Dies letztere ist aber genau dann wahr, wenn

$$A^{*2}z = -z.$$

$\mathfrak{L}$ besteht also genau aus den $\{z, A^*z\}$ mit $A^{*2}z = -z$.

2. Es ist nun unsere Aufgabe, alle hermiteschen abgeschlossenen Operatoren A', die Fortsetzungen von A sind ($A' \geqq A$), zu überblicken und insbesondere etwas über maximale oder gar selbstadjungierte Operatoren, die sich unter diesen A' befinden, auszusagen. Zu dem Zweck stellen wir eine eineindeutige Abbildung der Menge aller hermiteschen abgeschlossenen $A' \geqq A$ auf die Menge aller der Unterräume $\mathfrak{Z}$ von $\mathfrak{L}$, für die $V\mathfrak{Z} \perp \mathfrak{Z}$ gilt, her.

A' sei eine hermitesche abgeschlossene Fortsetzung von A, also

$$A \leqq A', \qquad A' \leqq A'^*.$$

Aus $A \leqq A'$ folgt dann noch

$$A'^* \leqq A^*,$$

zusammengefaßt:

$$\mathfrak{B}_A \leqq \mathfrak{B}_{A'} \leqq \mathfrak{B}_{A'^*} \leqq \mathfrak{B}_{A^*}.$$

Es sei

$$\mathfrak{Z} = \mathfrak{B}_{A'} \ominus \mathfrak{B}_A.$$

Dann ist

$$\mathfrak{Z} \leqq \mathfrak{B}_{A^*} \ominus \mathfrak{B}_A = \mathfrak{L},$$
$$V\mathfrak{Z} = V\mathfrak{B}_{A'} \ominus V\mathfrak{B}_A \leqq V\mathfrak{B}_{A'} = \mathfrak{R}^2 \ominus \mathfrak{B}_{A'^*},$$
$$V\mathfrak{Z} \perp \mathfrak{B}_{A'^*} \geqq \mathfrak{B}_{A'} \geqq \mathfrak{Z},$$
$$V\mathfrak{Z} \perp \mathfrak{Z}.$$

Damit ist jedem A' ein Unterraum $\mathfrak{Z}$ von $\mathfrak{L}$ mit $V\mathfrak{Z} \perp \mathfrak{Z}$ zugeordnet. Aus der Definition von $\mathfrak{Z}$ folgt aber

$$\mathfrak{B}_{A'} = \mathfrak{B}_A \oplus \mathfrak{Z},$$

deshalb ist A' durch $\mathfrak{Z}$ (immer bei festem A) eindeutig bestimmt. Es bleibt noch zu zeigen, daß jedem $\mathfrak{Z}$ auch wirklich ein A' entspricht.

Sei

$$\mathfrak{Z} \leqq \mathfrak{L}, \qquad V\mathfrak{Z} \perp \mathfrak{Z}.$$

Dann ist $\mathfrak{B}_A \oplus \mathfrak{Z}$ als Unterraum des Bildes $\mathfrak{B}_{A^*}$ von A^* nach § 3, **4** selbst Bild eines abgeschlossenen Operators A':

$$\mathfrak{B}_A \oplus \mathfrak{Z} = \mathfrak{B}_{A'}.$$

A' ist Fortsetzung von A, darum existiert A'^*. Und aus

$$\mathfrak{B}_A \perp V\mathfrak{B}_A (= \mathfrak{R}^2 \ominus \mathfrak{B}_{A^*}), \qquad \mathfrak{B}_A \perp \mathfrak{L} \geqq V\mathfrak{Z},$$
$$\mathfrak{Z} \perp \mathfrak{R}^2 \ominus \mathfrak{B}_{A^*} = V\mathfrak{B}_A, \qquad \mathfrak{Z} \perp V\mathfrak{Z}$$

folgt

$$\mathfrak{B}_{A'} = \mathfrak{B}_A \oplus \mathfrak{Z} \perp V\mathfrak{B}_A \oplus V\mathfrak{Z} = V\mathfrak{B}_{A'},$$

deshalb ist A' hermitesch.

3. Wir haben also zu jedem hermiteschen abgeschlossenen Operator A einen Raum $\mathfrak{L}$ und in ihm einen Imaginäroperator V, und wir haben die hermiteschen abgeschlossenen Fortsetzungen A' von A eineindeutig den Unterräumen $\mathfrak{Z}$ von $\mathfrak{L}$ mit $V\mathfrak{Z} \perp \mathfrak{Z}$ zugeordnet. Bei dieser Zuordnung entsprechen einander natürlich $A' = A$ und $\mathfrak{Z} = 0$. A ist maximal, wenn jedes $\mathfrak{Z} = 0$ ist; A ist selbstadjungiert, wenn $\mathfrak{B}_A = \mathfrak{B}_{A^*}$, d. h. wenn $\mathfrak{L} = 0$ ist.

Zu einer hermiteschen abgeschlossenen Fortsetzung A' gehört genau wie in § 10, **1** ein

$$\mathfrak{L}' = \mathfrak{B}_{A'^*} \ominus \mathfrak{B}_{A'}.$$

Wir können $\mathfrak{L}'$ einfach durch das zu A' gehörige $\mathfrak{Z}$ ausdrücken: Aus

$$\mathfrak{B}_{A'} = \mathfrak{B}_A \oplus \mathfrak{Z}$$

und

$$\mathfrak{B}_{A'^*} = \mathfrak{R}^2 \ominus V\mathfrak{B}_{A'} = \mathfrak{R}^2 \ominus V\mathfrak{B}_A \ominus V\mathfrak{Z} = \mathfrak{B}_{A^*} \ominus V\mathfrak{Z}$$

folgt

$$\mathfrak{L}' = \mathfrak{L} \ominus (V\mathfrak{Z} \oplus \mathfrak{Z}).$$

In der Sprechweise von § 9 heißt das: der Fortsetzung von A zu A' entspricht die Herstellung der ersten Normalform für V in einem Unterraum $\mathfrak{Z} \oplus V\mathfrak{Z}$ von $\mathfrak{L}$; dadurch wird die Frage nach der Struktur von V auf die Betrachtung von V in dem orthogonalen Komplement $\mathfrak{L} \ominus (\mathfrak{Z} \oplus V\mathfrak{Z})$ zurückgeführt. Als Anwendung ergibt sich: *Die Fortsetzung A' ist dann und nur dann maximal, wenn für Unterräume $\mathfrak{Z}'$ von $\mathfrak{L}'$ aus $V\mathfrak{Z}' \perp \mathfrak{Z}'$ folgt $\mathfrak{Z}' = 0$; A' ist selbstadjungiert, wenn $\mathfrak{L}' = 0$, d. h. wenn $\mathfrak{L} = \mathfrak{Z} \oplus V\mathfrak{Z}$.*

Die weitere Untersuchung muß nun eine Fallunterscheidung hinsichtlich des Grundkörpers Σ machen.

4. Im reellen Hilbertschen Raum ($\Sigma = R$) gibt es nach § 9, **5** stets eine selbstadjungierte Fortsetzung A'.

Im Hilbertschen Raum ($\Sigma = K$) sei wieder $\mathfrak{U}$ die Menge der $\{z, A^*z\}$ in $\mathfrak{L}$ mit $V\{z, A^*z\} = \{z, A^*z\}i$, das ist die Menge der $\{z, A^*z\}$ mit $A^*z = zi$ [33]); $\mathfrak{V}$ aber sei die Menge der $\{z, A^*z\}$ in $\mathfrak{L}$ mit $V\{z, A^*z\} = -\{z, A^*z\}i$, das ist die Menge der $\{z, A^*z\}$ mit $A^*z = -zi$ [33]). Wie in § 9, **6** sei

$$\operatorname{Dim} \mathfrak{U} = \mathfrak{m}, \qquad \operatorname{Dim} \mathfrak{V} = \mathfrak{n}.$$

Durch Projizieren in den Abszissenraum erkennt man [34]), daß $\mathfrak{m}$ auch die Dimension des Unterraums aller z mit $A^*z = zi$ und $\mathfrak{n}$ die Dimension des Unterraums aller z mit $A^*z = -zi$ ist. Das Zahlenpaar $\{\mathfrak{m}, \mathfrak{n}\}$ heißt der *Defektindex von A*. Aus § 9, **6** folgt: *Es gibt dann und nur dann eine hermitesche abgeschlossene Fortsetzung A' von A mit dem Defektindex $\{\mathfrak{m}', \mathfrak{n}'\}$, wenn es eine Kardinalzahl $\mathfrak{p}$ so gibt, daß*

$$\mathfrak{m} = \mathfrak{p} + \mathfrak{m}', \qquad \mathfrak{n} = \mathfrak{p} + \mathfrak{n}'$$ [35]).

In § 9, **6** haben wir die $\mathfrak{Z} \leq \mathfrak{L}$ mit $V\mathfrak{Z} \perp \mathfrak{Z}$, also die hermiteschen abgeschlossenen Fortsetzungen A' von A, eineindeutig den isometrischen Abbildungen S eines Unterraums $\mathfrak{N}$ von $\mathfrak{V}$ auf einen Unterraum $\mathfrak{M}$ von $\mathfrak{U}$ zugeordnet. Und zwar war $\mathfrak{Z}$ der Wertebereich von $E + S$, und für $\{z, A^*z\} \in \mathfrak{Z}$ war

$$V\{z, A^*z\} = i(S - E)(S + E)^{-1}\{z, A^*z\}.$$

Projiziert man diesen Sachverhalt in den Abszissenraum, so sieht man, wie hier nicht weiter ausgeführt werden soll, einen gewissen Zusammenhang mit der Cayleytransformation.

5. Im Wachsschen Raum ($\Sigma = Q$) setzen wir

$$\operatorname{Dim} \mathfrak{L} = \mathfrak{d}$$

und nennen $\mathfrak{d}$ den Defektindex von A. Nach § 9, **7** gibt es *dann und nur dann eine hermi-*

---

[33]) $\{z, A^* z\}$ liegt dann wegen $A^{*2} z = -z$ nach § 10, **1** von selbst in $\mathfrak{L}$.

[34]) Dies Projizieren ist bis auf den Faktor $\frac{1}{\sqrt{2}}$ eine isometrische Transformation. Man braucht also nicht den Beweis aus § 6, **2** heranzuziehen.

[35]) v. Neumann [1] VIII, Stone [1] S. 339.

tesche abgeschlossene Fortsetzung von A mit dem Defektindex $\mathfrak{d}$, *wenn es eine Kardinalzahl* $\mathfrak{p}$ *mit*

$$\mathfrak{d} = 2\mathfrak{p} + \mathfrak{d}'$$

gibt. Aus der Diskussion am Schluß von § 9, **7** liest man sofort ab:

$\mathfrak{d} = 0 \longleftrightarrow A$ selbstadjungiert.

$\mathfrak{d} = 1 \longleftrightarrow A$ nurmaximal.

$\mathfrak{d} \equiv 0 (\mathrm{mod}\ 2) \longleftrightarrow A$ selbstadjungiert fortsetzbar, nicht nurmaximal fortsetzbar.

$\mathfrak{d} \equiv 1 (\mathrm{mod}\ 2) \longleftrightarrow A$ nurmaximal fortsetzbar, nicht selbstadjungiert fortsetzbar.

$\mathfrak{d} \geqq \mathfrak{a} \longleftrightarrow A$ selbstadjungiert fortsetzbar und nurmaximal fortsetzbar.

Der Defektindex $\mathfrak{d}$ ist, wie Projizieren in den Abszissenraum lehrt, die Dimension der Menge aller z mit $A^{*2}z = -z$ (§ 6, **2**). Aus § 6, **5** folgt, daß $\mathfrak{d}$ nur von den Definitionsbereichen von A und A^*, nicht aber von der sonstigen Struktur dieser Operatoren abhängt. Insbesondere hat $\lambda A + \mu E$ ($\lambda, \mu \in R$; $\lambda \neq 0$) denselben Defektindex wie A. So ließen sich noch einige Sätze über hermitesche abgeschlossene Operatoren aus dem Hilbertschen Raum übertragen bzw. dort neu beweisen, wir wollen uns aber darauf beschränken, eine Übersicht über die nurmaximalen Operatoren im Wachsschen Raum zu geben.

§ 11. Nurmaximale Operatoren im Wachsschen Raum.

1. Zunächst soll bei vorläufig beliebigem Grundkörper Σ das Verhalten des in § 10, **1** eingeführten Unterraums $\mathfrak{L}$ bei Reduktion untersucht werden. Sei also A ein hermitescher abgeschlossener Operator, $\mathfrak{L} = \mathfrak{B}_{A^*} \ominus \mathfrak{B}_A$, P sei Projektor mit dem Wertbereich $\mathfrak{M}$, $\mathfrak{N} = \mathfrak{R} \ominus \mathfrak{M}$, es gelte $P \mathfrak{v} A$. Dann gilt nach § 4, **1** auch $P = P^* \mathfrak{v} A^*$. Nach § 4, **3** führt P die Unterräume $\mathfrak{B}_A$ und $\mathfrak{B}_{A^*}$ in sich über, ist also (§ 3, **3**) mit den zu $\mathfrak{B}_A$ und $\mathfrak{B}_{A^*}$ gehörigen Projektoren vertauschbar. Deshalb ist P auch mit dem zu $\mathfrak{L}$ gehörigen Projektor vertauschbar: P führt $\mathfrak{L}$ in sich über, und es ist

$$\mathrm{Dim}\,(\bar{P}\mathfrak{L}) + \mathrm{Dim}\,((\bar{E} - \bar{P})\,\mathfrak{L}) = \mathrm{Dim}\,\mathfrak{L}.$$

Betrachtet man nun aber A als hermiteschen abgeschlossenen Operator in $\mathfrak{M}$, so muß man in den Betrachtungen des § 10 offenbar $\mathfrak{R}^2$ durch $\mathfrak{M}^2 = \bar{P}\mathfrak{R}^2$, $\mathfrak{B}_A$ durch $\bar{P}\mathfrak{B}_A$, $\mathfrak{B}_{A^*}$ durch $\bar{P}\mathfrak{B}_{A^*}$ und mithin $\mathfrak{L} = \mathfrak{B}_{A^*} \ominus \mathfrak{B}_A$ durch $\bar{P}\mathfrak{B}_{A^*} \ominus \bar{P}\mathfrak{B}_A = \bar{P}\mathfrak{L}$ ersetzen. Entsprechendes gilt für $\bar{E} - \bar{P}$ und $\mathfrak{N}$. Damit sind also in der obigen Formel die beiden Unterräume auf der linken Seite geometrisch gedeutet.

Ist insbesondere $\mathfrak{R} = \mathfrak{W}$ ein Wachsscher Raum, so kann man sagen: *Der Defektindex von A ist die Summe der beiden Defektindizes, die A als in $\mathfrak{M}$ bzw. in $\mathfrak{N}$ erklärter hermitescher abgeschlossener Operator hat.*

2. A sei ein nurmaximaler Operator im Wachsschen Raum $\mathfrak{W}$, d. h. nach § 10, **5** ein hermitescher abgeschlossener Operator mit dem Defektindex $\mathfrak{d} = 1$. Dann gibt es nach § 8, **3** in $\mathfrak{L} = \mathfrak{B}_{A^*} \ominus \mathfrak{B}_A$ ein $\{z_0, A^*z_0\}$ mit $V\{z_0, A^*z_0\} = \{z_0, A^*z_0\}i$, das den Unterraum $\mathfrak{L}$ erzeugt. Oder: Es gibt ein $z_0 \neq 0$ in $\mathfrak{W}$ mit

$$A^*z_0 = z_0 i, \tag{1}$$

o. B. d. A. können wir

$$|z_0| = 1 \tag{2}$$

annehmen, und jedes z mit $A^{*2}z = -z$ ist von z_0 linear abhängig:

(3) Aus $A^{*2}z = -z$ folgt $z = z_0 a$ $(a \in Q)$.

Nach § 3, **4** ist

$$H = (A^*A + E)^{-1}$$

ein beschränkter hermitescher Operator; es sei

$$H^n z_0 = z_n \quad (n > 0),$$

also

$$A^*Az_n + z_n = z_{n-1} \quad (n > 0).$$

Insbesondere liegen die z_n $(n > 0)$ alle im Definitionsbereich von A. Wegen $A \subseteq A^*$ können wir natürlich auch schreiben

$$A^{*2}z_n + z_n = z_{n-1} \quad (n > 0). \tag{4}$$

(4) reicht aber nur in Verbindung damit, daß die z_n $(n > 0)$ im Definitionsbereich von A liegen, zur Definition der z_n aus.

Es werde definiert

$$(z_k, z_0) = b_k \quad (k \geqq 0).$$

Dann ist, weil H hermitesch und beschränkt ist,

$$(z_m, z_n) = (H^m z_0, H^n z_0) = (H^{m+n} z_0, z_0) = (z_{m+n}, z_0),$$

$$(z_m, z_n) = b_{m+n}, \tag{5}$$

insbesondere

$$\bar{b}_k = \overline{(z_k, z_0)} = (z_0, z_k) = b_k,$$

$$b_k \in R. \tag{6}$$

Nun gibt es Quaternionen a_k so, daß

$$A^*z_n = \sum_{\nu=0}^{n} z_\nu a_{n-\nu} \qquad (n \geqq 0). \tag{7}$$

Beweis durch Induktion: $n = 0$ mit $a_0 = i$ ist nach (1) klar. Es seien schon Quaternionen $a_0, a_1, \ldots, a_{n-1}$ bekannt derart, daß

$$A^*z_m = \sum_{\mu=0}^{m} z_\mu a_{m-\mu} \qquad (0 \leqq m \leqq n-1).$$

Setzt man dann

$$A^*z_n - \sum_{\nu=1}^{n} z_\nu a_{n-\nu} = z', \tag{8}$$

so folgt durch Anwenden von $A^{*2} + E$ unter Beachtung von (4)

$$(A^{*2} + E)z' = A^*z_{n-1} - \sum_{\nu=1}^{n} z_{\nu-1} a_{n-\nu} = A^*z_{n-1} - \sum_{\mu=0}^{n-1} z_\mu a_{n-1-\mu} = 0;$$

nach (3) gibt es ein $a_n \in Q$ mit

$$z' = z_0 a_n.$$

Setzt man dies in (8) ein, so steht (7) da.

Bildet man in (7) das innere Produkt mit z_0, so erhält man

$$\sum_{\nu=0}^{n} b_\nu a_{n-\nu} = (Az_n, z_0) = (z_n, A^*z_0) = (z_n, z_0 i) = -ib_n,$$

$$b_0 a_n + b_1 a_{n-1} + \cdots + b_{n-1} a_1 + b_n a_0 = -ib_n \ (n > 0). \tag{9}$$

Wendet man auf (7) andererseits A^* an und beachtet man (4) und (7), so folgt

$$z_{n-1} - z_n = \sum_{\nu=0}^{n} A^* z_\nu a_{n-\nu} = \sum_{\nu=0}^{n} \sum_{\mu=0}^{\nu} z_\mu a_{\nu-\mu} a_{n-\nu} \quad (n > 0). \tag{10}$$

Nun sind die z_n linear unabhängig. Denn wegen (2) ist $z_0 \neq 0$. Wäre

$$\sum_{\nu=0}^{n} z_\nu c_\nu = 0, \qquad c_n \neq 0, \qquad 0 < n = \text{Min.},$$

so würde durch Anwenden von $A^{*2} + E$ folgen

$$\sum_{\nu=1}^{n} z_{\nu-1} c_\nu = 0, \qquad c_n \neq 0$$

im Widerspruch zur Voraussetzung $n = \text{Min}$. Daher sind in (10) die Koeffizienten von

z_0 auf beiden Seiten gleich:

$$(11) \qquad \sum_{\nu=0}^{n} a_\nu\, a_{n-\nu} = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases} \qquad (n > 0).$$

Nun folgt aus (9) durch Induktion, weil die b_k nach (6) reell sind und nach (2) $b_0 = 1$ ist, daß

$$a_n \in K.$$

Alle a_n sind miteinander vertauschbar. Deshalb kann (11) zur rekursiven Berechnung der a_n verwandt werden, der Koeffizient von a_n in (11) ist ja $2a_0 = 2i \neq 0$. Jetzt kann man analog aus (9) rekursiv die b_n berechnen. Die Gleichungen (11) und (9) sind aber von A frei. Darum hängen die a_n und die b_n nur von ihrem Index n, nicht aber von der speziellen Wahl des nurmaximalen Operators A ab [36]).

3. Der Definitionsbereich von A heiße $\mathfrak{D}$. Es sei $\mathfrak{M}$ der von $z_0, z_1, \ldots, z_n, \ldots$ erzeugte Unterraum, $\mathfrak{W} \ominus \mathfrak{M} = \mathfrak{N}$. Es soll bewiesen werden: $\mathfrak{M}$ reduziert A. Zu dem Zweck bezeichnen wir mit $\mathfrak{B}'$ den von $\{z_1, Az_1\}, \{z_2, Az_2\}, \ldots$ erzeugten Unterraum in $\mathfrak{B}_A$. Ferner erklären wir $\mathfrak{D}_1$ und $\mathfrak{D}_2$ durch

$$\{\mathfrak{D}_1, 0\} = F\mathfrak{B}', \qquad \mathfrak{D}_2 = \mathfrak{D} \cap \mathfrak{N}.$$

Dann ist (nach Definition der Reduktion in § 4, 2) zu zeigen:

1. $A\mathfrak{D}_1 \leqq \mathfrak{M}$.
2. $A\mathfrak{D}_2 \leqq \mathfrak{N}$.
3. $\mathfrak{D} = \mathfrak{D}_1 \dotplus \mathfrak{D}_2$.

Beweis. 1. Nach Definition von $\mathfrak{D}_1$ ist

$$\{0, A\mathfrak{D}_1\} = (\overline{E} - F)\mathfrak{B}'.$$

Weil die $\{z_n, Az_n\}$ $(n > 0)$ eine Grundmenge in $\mathfrak{B}'$ sind, sind die Az_n eine Grundmenge in $A\mathfrak{D}_1$. Nach (7) liegen aber alle Az_n $(n > 0)$ in $\mathfrak{M}$.

2. Gilt $(y, z_n) = 0$ für alle $n \geqq 0$, so ist auch

$$(Ay, z_n) = (y, A^* z_n) = \Big(y, \sum_{\nu=0}^{n} z_\nu\, a_{n-\nu}\Big) = 0,$$

wenn Ay existiert; aus $y \in \mathfrak{D} \cap \mathfrak{N}$ folgt also $Ay \perp \mathfrak{M}$, $Ay \in \mathfrak{N}$.

3. Für alle $y \in \mathfrak{D}$ gilt die Identität

$$(\{y, Ay\}, \{z_n, Az_n\}) = (y, z_n) + (Ay, Az_n) = (y, z_n + A^*Az_n) = (y, z_{n-1}) \qquad (n > 0).$$

Verschwinden der linken Seite bedeutet $\{y, Ay\} \in \mathfrak{B}_A \ominus \mathfrak{B}'$, Verschwinden der rechten Seite bedeutet $y \in \mathfrak{D}_2$. Es ist also

$$\{\mathfrak{D}_2, 0\} = F(\mathfrak{B}_A \ominus \mathfrak{B}').$$

Aus

$$\mathfrak{B}_A = \mathfrak{B}' \oplus (\mathfrak{B}_A \ominus \mathfrak{B}')$$

folgt demnach durch Anwenden von F

$$\{\mathfrak{D}, 0\} = \{\mathfrak{D}_1, 0\} \dotplus \{\mathfrak{D}_2, 0\},$$
$$\mathfrak{D} = \mathfrak{D}_1 \dotplus \mathfrak{D}_2.$$

4. Weil z_0 in $\mathfrak{M}$ liegt, kann A in $\mathfrak{M}$ nicht selbstadjungiert sein, A muß in $\mathfrak{M}$ mindestens den Defektindex 1 haben. A hat aber in ganz $\mathfrak{W}$ den Defektindex 1, und nach § 11, 1 verhält sich der Defektindex bei Reduktion additiv. Das ist nur möglich, wenn A in $\mathfrak{M}$ den Defektindex 1 und in $\mathfrak{N}$ den Defektindex 0 hat. Wir wollen noch zeigen, daß $\mathfrak{N}$ der größte A reduzierende Unterraum ist, in dem A selbstadjungiert ist, daß also A in $\mathfrak{M}$ irreduzibel ist.

---

[36]) Es ist $a_n = (-1)^n \binom{\frac{1}{2}}{n} i$, $b_n = 2(-1)^n \binom{\frac{1}{2}}{n+1}$.

Sei P ein Projektor, $P \mathfrak{v} A$. Dann hat wie oben A in $P\mathfrak{W}$ oder in $(E - P)\mathfrak{W}$, o. B. d. A. in $P\mathfrak{W}$, den Defektindex 1, im orthogonalen Komplement $(E - P)\mathfrak{W}$ den Defektindex 0. $P\mathfrak{W}$ enthält also ein $z \neq 0$ mit $(A^{*2} + E)z = 0$, das nach (3) von z_0 linear abhängig ist, d. h. $P\mathfrak{W}$ enthält z_0. Aus $P \mathfrak{v} A$ folgt nun $P \mathfrak{v} A^*$, $P \mathfrak{v} (A^*A + E)^{-1} = H$, $P\mathfrak{W}$ reduziert H, $P\mathfrak{W}$ enthält mit z_0 auch alle $H^n z_0 = z_n$, d. h. $\mathfrak{M} \subseteq P\mathfrak{W}$.

Der nurmaximale Operator A legt also eindeutig eine Zerlegung

$$\mathfrak{W} = \mathfrak{M} \oplus \mathfrak{N}$$

des Raumes $\mathfrak{W}$ fest derart, daß A in $\mathfrak{M}$ irreduzibel und nurmaximal, in $\mathfrak{N}$ dagegen selbstadjungiert ist. Natürlich ist

$$\mathrm{Dim}\, \mathfrak{M} = \mathfrak{a}.$$

5. A und B seien zwei irreduzible nurmaximale Operatoren im Wachsschen Raum $\mathfrak{W}$. (Dann ist $\mathrm{Dim}\, \mathfrak{W} = \mathfrak{a}$.) Wie in § 11, 2 seien $z_0, z_1, \ldots$ so gewählt, daß $|z_0| = 1$, $A^* z_0 = z_0 i$, $(A^*A + E)^{-n} z_0 = z_n$. Analog seien $\zeta_0, \zeta_1, \ldots$ so gewählt, daß $|\zeta_0| = 1$, $B^* \zeta_0 = \zeta_0 i$, $(B^*B + E)^{-n} \zeta_0 = \zeta_n$. Nach dem E. Schmidtschen Orthogonalisierungsverfahren kann man aus $z_0, z_1, \ldots$ ein Orthonormalsystem $p_0, p_1, \ldots$ herstellen, das durch die beiden Eigenschaften

1. p_n ist von $z_0, z_1, \ldots, z_n$ linear abhängig,
2. $(p_n, z_n) > 0$

eindeutig bestimmt ist [37]). In

$$p_n = \sum_{\nu=0}^{n} z_\nu c_{\nu n}, \qquad z_n = \sum_{\nu=0}^{n} p_\nu d_{\nu n}$$

sind dann die $c_{\nu n}$ und die $d_{\nu n}$ nur von den b_k abhängig; weil aber die b_k nach § 11, 2 nicht von A abhängen, sind auch die $c_{\nu n}$ und die $d_{\nu n}$ nur von ν und n, nicht aber von A abhängig. Konstruiert man das Orthonormalsystem $q_0, q_1, \ldots$ zu $\zeta_0, \zeta_1, \ldots$ genau so wie $p_0, p_1, \ldots$ zu $z_0, z_1, \ldots$, so ist deshalb

$$q_n = \sum_{\nu=0}^{n} \zeta_\nu c_{\nu n}, \qquad \zeta_n = \sum_{\nu=0}^{n} q_\nu d_{\nu n}$$

mit denselben $c_{\nu n}$ und $d_{\nu n}$. Der von $p_0, p_1, \ldots$ erzeugte Unterraum ist genau der von $z_0, z_1, \ldots$ erzeugte Unterraum, dieser reduziert A nach § 11, 3; weil A als irreduzibel vorausgesetzt war, ist jener Unterraum gleich $\mathfrak{W}$: die $p_0, p_1, \ldots$ sind ein in $\mathfrak{W}$ vollständiges Orthonormalsystem. Analog sind die $q_0, q_1, \ldots$ ein in $\mathfrak{W}$ vollständiges Orthonormalsystem, weil B irreduzibel ist. Darum gibt es einen unitären Operator U mit

$$q_n = U p_n \qquad (n \geqq 0).$$

Dann ist auch

$$\zeta_n = \sum_{\nu=0}^{n} q_\nu d_{\nu n} = \sum_{\nu=0}^{n} U p_\nu d_{\nu n} = U z_n$$

und

$$B\zeta_n = \sum_{\nu=0}^{n} \zeta_\nu a_{n-\nu} = \sum_{\nu=0}^{n} U z_\nu a_{n-\nu} = UAz_n = UAU^{-1} \zeta_n \qquad (n > 0),$$

denn in (7) sind auch die a_k von der speziellen Wahl von A unabhängig. Dem Beweis in § 11, 3 entnimmt man, daß $\mathfrak{B}_A$ der von den $\{z_1, Az_1\}, \{z_2, Az_2\}, \ldots$ erzeugte Unterraum ist. Das orthogonale Komplement dieses Unterraums in $\mathfrak{B}_A$ entsprach ja dem dortigen $\mathfrak{N}$, das hier verschwindet. Analog ist $\mathfrak{B}_B$ der von den $\{\zeta_1, B\zeta_1\}, \{\zeta_2, B\zeta_2\}, \ldots$ erzeugte Unterraum. Aus

$$\{\zeta_n, B\zeta_n\} = \overline{U}\{z_n, Az_n\} \qquad (n > 0)$$

[37]) Weil die z_n linear unabhängig sind.

folgt darum

$$\mathfrak{B}_B = \bar{U}\mathfrak{B}_A .$$

Dies ist aber offensichtlich gleichbedeutend mit

$$B = UAU^{-1}.$$

Also: *Alle nurmaximalen irreduziblen Operatoren im Wachsschen Raum sind unitäräquivalent.*

6. Man kann schließlich noch die Frage aufwerfen: Gibt es überhaupt nurmaximale Operatoren im unendlichdimensionalen Wachsschen Raum? Das ist tatsächlich der Fall. Man stelle sich z. B. einen maximalen Hilbertschen Teilraum $\mathfrak{H}$ des Wachsschen Raums $\mathfrak{W}$ wie in § 8, **3** her (etwa als abgeschlossene Hülle des von einem in $\mathfrak{W}$ vollständigen Orthonormalsystem erzeugten K-Rechtsmoduls), in diesem kann man dann einen nurmaximalen Operator vom Defektindex $\{1, 0\}$ konstruieren [38]). Dieser wird sich in eindeutig bestimmter Weise zu einem nurmaximalen Operator des Wachsschen Raums $\mathfrak{W}$ fortsetzen.

Man kann auch einen nurmaximalen Operator im Funktionenraum explizit hinschreiben [39]).

§ 12. Propädeutische Betrachtung normaler Operatoren.

1. Ein abgeschlossener Operator N heißt *normal*, wenn N^* existiert und wenn

$$NN^* = N^*N \text{ [40])}$$

oder, was dasselbe ist,

$$(NN^* + E)^{-1} = (N^*N + E)^{-1}.$$

Z. B. ist jeder selbstadjungierte Operator und jeder Imaginäroperator normal. Im Hilbertschen Raum gibt es bekanntlich eine Spektralzerlegung normaler Operatoren [41]), die sich von der Spektralzerlegung selbstadjungierter Operatoren im wesentlichen nur dadurch unterscheidet, daß sich das Spektrum über die ganze Gaußsche Ebene erstrecken kann. Ein Analogon im Wachsschen Raum ist nicht ohne weiteres zu sehen. Deshalb wollen wir uns erst am Spezialfall des endlichdimensionalen Wachsschen Raums orientieren, um zu erfahren, was wir im allgemeinen Fall erwarten dürfen.

2. Ist $p_1, p_2, \ldots, p_n$ ein vollständiges Orthonormalsystem im n-dimensionalen Wachsschen Raum $\mathfrak{W}$ und sind $\lambda_1, \lambda_2, \ldots, \lambda_n$ beliebige Quaternionen, so wird durch

$$Np_\nu = p_\nu \lambda_\nu \qquad (\nu = 1, 2, \ldots, n) \tag{1}$$

ein beschränkter Operator N festgelegt, der offenbar normal ist. Aber $\lambda_1, \lambda_2, \ldots, \lambda_n$ sind durch N nicht bis auf die Reihenfolge eindeutig bestimmt. Wenn man z. B. p_1 durch $p_1\eta$ ersetzt ($|\eta| = 1$) und $p_2, \ldots, p_n$ ungeändert läßt, so muß man, damit (1) auch nach dieser Transformation gilt, λ_1 durch $\eta^{-1}\lambda_1\eta$ ersetzen, was für $\lambda_1 \notin R$ im allgemeinen von λ_1 verschieden ist, während sich $\lambda_2, \ldots, \lambda_n$ nicht ändern. Die $\lambda_1, \ldots, \lambda_n$ lassen sich nun bekanntlich durch solche Transformationen $\lambda \to \eta^{-1}\lambda\eta$ ($|\eta| = 1$) alle in die abgeschlossene obere Halbebene von K bringen, so daß für die transformierten $\lambda_1, \ldots, \lambda_n$ gilt

$$\lambda_\nu \in K, \quad \frac{\lambda_\nu - \bar{\lambda}_\nu}{2i} \geqq 0. \tag{2}$$

Wir dürfen also immer annehmen, in (1) seien die $\lambda_1, \ldots, \lambda_n$ schon gemäß (2) gewählt. Unter dieser Zusatzvoraussetzung läßt sich nun leicht zeigen, daß die λ_ν durch

[38]) Z. B. Stone [1] S. 349f.

[39]) Vgl. Stone [1], Theorem 10.8.

[40]) In bezug auf den Sinn dieser Definition siehe v. Neumann [3] S. 308f.

[41]) v. Neumann [2] V, Stone [1] VIII § 3.

N bis auf die Reihenfolge eindeutig bestimmt sind: Ist $q_1, \ldots, q_n$ noch ein Orthonormalsystem,

$$Nq_\varrho = q_\varrho \mu_\varrho \quad (\varrho = 1, \ldots, n),$$

$$\mu_\varrho \in K, \quad \frac{\mu_\varrho - \bar{\mu}_\varrho}{2i} \geqq 0,$$

und ist etwa

$$q_1 = \sum_{\nu=1}^{n} p_\nu \xi_\nu,$$

so ist

$$\sum_{\nu=1}^{n} p_\nu \lambda_\nu \xi_\nu = Nq_1 = q_1 \mu_1 = \sum_{\nu=1}^{n} p_\nu \xi_\nu \mu_1,$$

$$\lambda_\nu \xi_\nu = \xi_\nu \mu_1;$$

aus $\lambda_\nu = \xi_\nu \mu_1 \xi_\nu^{-1}$ folgt wegen der eindeutigen Normierung (2) der λ_ν und μ_ϱ, daß $\lambda_\nu = \mu_1$, daher ist $\xi_\nu = 0$ für $\lambda_\nu \neq \mu_1$; jedes q_ϱ ist daher von den p_ν mit

$$\lambda_\nu = \mu_\varrho$$

linear abhängig, zu einem jeden „Eigenwert“ λ gibt es höchstens so viele q_ϱ wie p_ν, weil doch diese q_ϱ in dem durch diese p_ν bestimmten Unterraum ein Orthonormalsystem sind; es gibt aber gleich viele q_ϱ wie p_ν (nämlich n), daraus folgt die Behauptung.

3. *Jeder normale Operator N im n-dimensionalen ($n < \mathfrak{a}$) Wachsschen Raum läßt sich in der Hauptachsenform* (1) *darstellen.*

Beweis (durch Induktion nach n). Der beschränkte hermitesche Operator $N + N^*$ hat nach § 8, 4 einen reellen Eigenwert:

$$(N + N^*)p = \lambda p, \quad p \neq 0, \quad \lambda \in R.$$

Der zum Unterraum $\mathfrak{M}$ aller p mit

$$(N + N^*)p = \lambda p$$

gehörende Projektor ist nach der Spektraltheorie wegen $N \mathfrak{v} N + N^*$ mit N vertauschbar: $\mathfrak{M}$ reduziert N. Genau so reduziert der Unterraum $\mathfrak{M} \neq 0$ den beschränkten hermiteschen Operator

$$\left(N - \frac{\lambda}{2} E\right)^* \left(N - \frac{\lambda}{2} E\right);$$

dieser Operator hat also einen (natürlich nichtnegativen) Eigenwert μ, auch wenn man ihn nur als Operator in $\mathfrak{M}$ betrachtet:

$$\left(N - \frac{\lambda}{2} E\right)^* \left(N - \frac{\lambda}{2} E\right) p = \mu p, \qquad p \neq 0 \text{ in } \mathfrak{M}, \ \mu \geqq 0 \text{ in } R.$$

Wegen $N \mathfrak{v} \left(N - \frac{\lambda}{2} E\right)^* \left(N - \frac{\lambda}{2} E\right)$ reduziert der Unterraum $\mathfrak{N}$ aller p mit

$$\text{(3)} \qquad \begin{cases} (N + N^*)\, p = \lambda p, \\ \left(N - \frac{\lambda}{2} E\right)^* \left(N - \frac{\lambda}{2} E\right) p = \mu p \end{cases}$$

gleichfalls N. Ist nun

$$\mu > 0,$$

so reduziert $\mathfrak{N}$ auch den Operator

$$T = \frac{N - \frac{\lambda}{2} E}{\sqrt{\mu}}.$$

Dieser Operator T ist aber, als Operator nur in $\mathfrak{N}$ betrachtet, Imaginäroperator: (3) besagt ja genau

$$(T + T^*)\, p = 0, \qquad T^* T p = p$$

für alle $p \in \mathfrak{N}$. Nach § 8, **3** gibt es ein in $\mathfrak{N}$ vollständiges Orthonormalsystem $p_1, \ldots, p_s$ mit

$$T p_\nu = P_\nu i \qquad (\nu = 1, \ldots, s),$$

d. h.

$$N p_\nu = p_\nu \left(\frac{\lambda}{2} + \sqrt{\mu}\, i\right). \tag{4}$$

Sollte aber $\mu = 0$ sein, so folgt aus (3)

$$\left(\left(N - \frac{\lambda}{2} E\right)^* \left(N - \frac{\lambda}{2} E\right) p, p\right) = 0,$$

$$\left(N - \frac{\lambda}{2} E\right) p = 0.$$

(4) ist dann für jedes beliebige vollständige Orthonormalsystem $p_1, \ldots, p_s$ in $\mathfrak{N}$ erfüllt. Um (1) zu erreichen, genügt es nun, $p_1, \ldots, p_s$ durch ein geeignetes vollständiges Orthonormalsystem in $\mathfrak{W} \ominus \mathfrak{N}$ zu ergänzen, d. h. N in $\mathfrak{W} \ominus \mathfrak{N}$ auf die Form (1) zu bringen. Wegen $\mathfrak{N} \neq 0$ ist aber

$$\mathrm{Dim}(\mathfrak{W} \ominus \mathfrak{N}) < \mathrm{Dim}\, \mathfrak{W} = n.$$

Setzen wir die Lösbarkeit von (1) für alle kleineren Dimensionen als n voraus, so folgt sie auch für n.

Man beachte, daß wir (2) gleich nebenher erreicht haben. Der Grundgedanke dieses Beweises ist derselbe wie der des Beweises des Hauptsatzes in § 13.

4. Nehmen wir einmal der Einfachheit halber an, in (1), (2) seien alle

$$\frac{\lambda_\nu - \bar{\lambda}_\nu}{2i} > 0,$$

also kein λ_ν reell. Dann ist der durch

$$T_0 p_\nu = p_\nu i \qquad (\nu = 1, \ldots, n)$$

festgelegte Imaginäroperator T_0 mit N vertauschbar, und jeder mit N vertauschbare beschränkte Operator ist auch mit T_0 vertauschbar [42]). In den Bezeichnungen des letzten Beweises stimmt T_0 mit dem damals eingeführten T genau in $\mathfrak{N}$ überein. Setzt man

$$\lambda_\nu = \lambda'_\nu + i\lambda''_\nu, \quad \lambda'_\nu \in R, \quad 0 < \lambda''_\nu \in R,$$

so geht (1) in

$$N p_\nu = (\lambda'_\nu E + \lambda''_\nu T_0)\, p_\nu \qquad (\nu = 1, \ldots, n)$$

über. Dies ist die vernünftige Schreibweise und nicht (1); das sieht man schon daran, daß für festes λ' und λ'' die Menge der p mit

$$N p = (\lambda' E + \lambda'' T_0)\, p$$

ein Unterraum ist, während doch bei festem $\lambda \notin R$ die Menge der p mit

$$N p = p\lambda$$

kein Unterraum war. Man muß also sozusagen das i als T_0 nach vorn ziehen, was nur für gewisse p erlaubt ist, und erhält eine Gleichung mit größerem, abgeschlossenerem

---

[42]) Aus $\lambda_\alpha c_{\alpha\beta} = c_{\alpha\beta} \lambda_\beta$, $\lambda_\nu \in K$, $\frac{\lambda_\nu - \bar{\lambda}_\nu}{2i} > 0$ folgt $i c_{\alpha\beta} = c_{\alpha\beta} i$ oder $c_{\alpha\beta} = 0$.

Gültigkeitsbereich. Wie sich aus den nachfolgenden Erörterungen ergeben wird, ist T_0 durch N eindeutig und unitärinvariant bestimmt.

Jetzt können wir schon ungefähr formulieren, was bei unendlicher Dimension zu erwarten ist. Wir werden eine Spektralzerlegung normaler Operatoren erhalten, ähnlich der im Hilbertschen Raum, nur wird das gesamte Spektrum bei geeigneter Normierung der abgeschlossenen oberen Halbebene angehören. Und was im Hilbertschen Raum i tat, wird im Wachsschen Raum ein geeigneter Imaginäroperator T_0 tun.

Was geschieht aber, wenn die Voraussetzung $\frac{\lambda_\nu - \bar{\lambda}_\nu}{2i} > 0$ nicht mehr für alle $\nu = 1, 2, \ldots, n$ erfüllt ist? Nun, die p_ν mit $\frac{\lambda_\nu - \bar{\lambda}_\nu}{2i} > 0$ erzeugen jedenfalls einen Unterraum $\mathfrak{R}$, der N reduziert. Sein orthogonales Komplement $\mathfrak{W} \ominus \mathfrak{R}$ wird von den p_ν mit reellen λ_ν erzeugt, in $\mathfrak{W} \ominus \mathfrak{R}$ ist also N selbstadjungiert. Man erkennt leicht, daß $\mathfrak{W} \ominus \mathfrak{R}$ genau die Menge aller x mit

$$Nx = N^*x$$

ist. Einem selbstadjungierten Operator auch einen Imaginäroperator zuzuordnen, wäre unnütz; die Zuordnung könnte auch gar nicht unitärinvariant sein. Man wird daher den Imaginäroperator T_0 einfach nur in $\mathfrak{R}$ definieren.

Nun sind wir so weit, daß wir den Hauptsatz über normale Operatoren, dessen Beweis der Schluß dieser Arbeit gewidmet ist, endgültig formulieren können.

5. In Anbetracht der zuletzt erwähnten Schwierigkeit führen wir folgende *Bezeichnung* ein:

Ist C ein Operator und $\mathfrak{R}$ ein Unterraum und nimmt C im Durchschnitt seines Definitionsbereichs mit $\mathfrak{R}$ nur Werte aus $\mathfrak{R}$ an (z. B. wenn $\mathfrak{R}$ den Operator C reduziert), so bezeichnen wir mit $C_\mathfrak{R}$ den aus C durch Einengen des Definitionsbereichs von C auf seinen Durchschnitt mit $\mathfrak{R}$ entstehenden Operator. Also:

$$C_\mathfrak{R}\, x \begin{cases} = Cx, \text{ wenn } x \in \mathfrak{R} \text{ und } Cx \text{ sinnvoll,} \\ \text{sonst sinnlos.} \end{cases}$$

Dann gilt der

Hauptsatz über normale Operatoren: *N sei ein normaler Operator im Raum $\mathfrak{R}$. Dann gibt es zu N drei Operatoren A, B, T_0 und einen Unterraum $\mathfrak{R}$ mit folgenden Eigenschaften:*

a) *A und B sind selbstadjungierte Operatoren, B ist nichtnegativ definit; $\mathfrak{R}$ ist die abgeschlossene Hülle des Wertebereichs von B, also*[43]) *das orthogonale Komplement des Eigenraums von B zum Eigenwert 0; T_0 ist nur in $\mathfrak{R}$ erklärt und nimmt nur Werte aus $\mathfrak{R}$ an; T_0 ist, als Operator in $\mathfrak{R}$ angesehen, Imaginäroperator.*

b) *Jeder Spektralprojektor von A oder von B ist mit N und N^* vertauschbar; $\mathfrak{R}$ reduziert N und N^*, und in $\mathfrak{R}$ gilt $T_0 \mathfrak{v} N_\mathfrak{R}$, $T_0 \mathfrak{v} (N^*)_\mathfrak{R}$.*

c) *Ist C ein beschränkter Operator und gilt $C \mathfrak{v} N$ und $C \mathfrak{v} N^*$, so gilt $C \mathfrak{v} A$, $C \mathfrak{v} B$, $\mathfrak{R}$ reduziert C, $C_\mathfrak{R} \mathfrak{v} T_0$ in $\mathfrak{R}$.*

d)
$$N = A + T_0 B,$$
$$N^* = A - T_0 B.$$

Der Hauptsatz soll in §§ 13—14 bewiesen werden. Es wird sich dabei auch die eindeutige Bestimmtheit von A, B, T_0, $\mathfrak{R}$ ergeben.

6. Ist $P_{\lambda'}$ die Spektralschar von A (d. h. ist $P_{\lambda'}$ der 0-Projektor von $A - \lambda' E$ im

[43]) Nach einer schon in § 3, **2** gemachten Bemerkung.

Sinne von § 7, 1) und ist $Q_{\lambda''}$ die Spektralschar von B, so folgt aus

$$N = A + T_0 B, \qquad A = \int_{-\infty}^{+\infty} \lambda' dP_{\lambda'}, \qquad B = \int_0^{\infty} \lambda'' dQ_{\lambda''}$$

formal

$$N = \int_{-\infty}^{+\infty} \int_0^{\infty} (\lambda' + T_0 \lambda'') dQ_{\lambda''} \, dP_{\lambda'},$$

d. h. eine Spektralzerlegung von N in der abgeschlossenen oberen Halbebene der Gaußschen Ebene, wo nur i durch T_0 ersetzt ist. Wir werden darauf noch genauer einzugehen haben, vorläufig begnügen wir uns mit der Feststellung, daß wirklich die $P_{\lambda'}$ mit den $Q_{\lambda''}$ vertauschbar sind [$P_{\lambda'} \mathfrak{v} N$, N^* nach b), darum $P_{\lambda'} \mathfrak{v} B$ nach c), d. h. $P_{\lambda'} \mathfrak{v} Q_{\lambda''}$] und daß aus ähnlichen Gründen auch $P_{\lambda' \mathfrak{R}}$ und $Q_{\lambda'' \mathfrak{R}}$ mit T_0 in $\mathfrak{R}$ vertauschbar sind.

Eine gewisse Analogie zu dem einfacheren lokalen Zerlegungssatz in § 7 ist unverkennbar: Erst Aussagen über die Natur der Dinge, deren Existenz behauptet wird [dort, daß P_- Projektor ist, hier a)], dann Vertauschbarkeit des neu Eingeführten mit dem Gegebenen [dort 2., hier b)], dann Vertauschbarkeit des Neuen mit allen beschränkten Operatoren C, die mit dem Gegebenen vertauschbar sind [dort 1., hier c); daß $\mathfrak{R}$ einen Operator reduziert, ist ja nach § 4, 2 auch eine Vertauschbarkeitsaussage], zuletzt die formale Relation, die das eigentliche Ziel der ganzen Konstruktion ist, ohne jene vorhergehenden Feststellungen aber praktisch wertlos wäre [dort 3. und 4., hier d)]; in § 7 schloß sich dann nur noch eine unwesentliche Normierung 5. an.

Es ist nach dem Vorangegangenen leicht, den Hauptsatz im Fall des endlichdimensionalen Wachsschen Raums direkt zu beweisen: Bringt man wieder N auf die Normalform (1), (2) und setzt man

$$\lambda_\nu = \lambda'_\nu + i\lambda''_\nu; \quad \lambda'_\nu, \lambda''_\nu \in R,$$

so werden A, B, T_0 durch

$$Ap_\nu = \lambda'_\nu p_\nu; \quad Bp_\nu = \lambda''_\nu p_\nu; \quad T_0 p_\nu = p_\nu i \qquad (\lambda''_\nu > 0)$$

bestimmt, während $\mathfrak{R}$ der von den p_ν mit $\lambda''_\nu > 0$ erzeugte Unterraum ist. Wir wollen aber auf die Einzelheiten nicht eingehen.

7. Der Hauptsatz gilt nicht nur im Wachsschen Raum, sondern auch in den beiden Hilbertschen Räumen. Es wird später klar werden, inwiefern er mit dem bekannten Spektralsatz für normale Operatoren im Hilbertschen Raum gleichwertig ist.

Wir werden in § 13 zuerst den Hauptsatz im Fall beschränkter normaler Operatoren direkt beweisen. Darauf werden wir ihn in drei einzelne Behauptungen zerlegen. In § 14 wird dann gezeigt, daß für jeden normalen Operator, für den jene drei Behauptungen zutreffen, auch der Hauptsatz gilt. Weil der Hauptsatz und damit auch die drei Behauptungen für beschränkte Operatoren schon bewiesen sein werden, wird es dann unsere einzige Aufgabe sein, sie von beschränkten auf unbeschränkte Operatoren zu übertragen; dies wird ähnlich wie in § 7, 3 geschehen. Es ist zwar durchaus möglich, den Hauptsatz direkt von beschränkten auf beliebige normale Operatoren zu übertragen, die hierbei notwendigen Rechnungen sind jedoch so wenig durchsichtig, daß der oben skizzierte Umweg bei weitem den Vorzug verdient, um so mehr, als er gerade an den praktischen spektraltheoretischen Anwendungen unserer vielleicht etwas ungewohnten und umständlichen Begriffsbildungen vorbeiführt. Die Kenntnis der gewöhnlichen Spektraltheorie, insbesondere ihres Rießschen Aufbaus [44]), wird dabei natürlich vorausgesetzt.

[44]) Rieß [1], bes. S. 45—51.

§ 13. Beschränkte normale Operatoren.

1. N sei ein beschränkter normaler Operator. Wir wollen den in § 12, **5** formulierten Hauptsatz für N beweisen, indem wir A, B, T_0, $\mathfrak{N}$ direkt angeben und die dort behaupteten Eigenschaften nachweisen.

Es werde definiert

$$A = \frac{N + N^*}{2}.$$

Dann ist A ein beschränkter selbstadjungierter Operator, und aus $C \mathfrak{v} N$, $C \mathfrak{v} N^*$ folgt $C \mathfrak{v} A$. Insbesondere gilt

$$A \mathfrak{v} N, N^*.$$

Darum ist auch jeder Spektralprojektor von A mit N und N^* vertauschbar.

Der Operator

$$(N - A)^*(N - A)$$

ist beschränkt, selbstadjungiert und nichtnegativ definit. Nach einer Bemerkung in § 3, **3** gibt es daher einen beschränkten selbstadjungierten nichtnegativ definiten Operator B mit den Eigenschaften: Es gilt

$$B^2 = (N - A)^*(N - A),$$

und aus $C \mathfrak{v} (N - A)^*(N - A)$ folgt $C \mathfrak{v} B$. Insbesondere folgt $C \mathfrak{v} B$ aus $C \mathfrak{v} N, N^*$, daher ist B und somit auch jeder Spektralprojektor von B mit N, N^*, A vertauschbar, denn N, N^*, A sind ja beschränkte mit N, N^* vertauschbare Operatoren.

$\mathfrak{N}$ sei der vom Wertebereich von B erzeugte Unterraum, also [43]) das orthogonale Komplement in $\mathfrak{R}$ des Unterraums aller x mit $Bx = 0$. Aus der Spektraltheorie ist bekannt, daß der zu $\mathfrak{N}$ gehörige Projektor genau der 0-Projektor von $-B$ ist (B war ja nichtnegativ definit). Aus $C \mathfrak{v} B$ folgt also, daß der zu $\mathfrak{N}$ gehörige Projektor mit C vertauschbar ist, d. h. daß $\mathfrak{N}$ den Operator C reduziert. Ist insbesondere der beschränkte Operator C mit N und N^* vertauschbar, so ist C, wie wir schon wissen, mit B vertauschbar, $\mathfrak{N}$ reduziert also alle diese C. Daher reduziert $\mathfrak{N}$ auch N und N^*.

Damit sind schon alle Behauptungen des Hauptsatzes bewiesen, in denen T_0 nicht vorkommt.

2. Nach Definition von B gilt identisch

$$|Bx| = |(N - A)x|.$$

Aus $Bx = 0$ folgt daher $(N - A)x = 0$. Zu jedem y gibt es deshalb höchstens ein z, mit dem für passendes x gilt:

$$Bx = y, \ (N - A)x = z.$$

Wäre nämlich etwa noch

$$Bx' = y, \ (N - A)x' = z',$$

so wäre

$$\begin{aligned} B(x - x') &= 0, \\ (N - A)(x - x') &= 0, \\ z &= z'. \end{aligned}$$

Der Operator, der genau den y, zu denen es solch ein z gibt, dies z zuordnet, während er den anderen y nichts zuordnet, heiße T':

$$T'y = z.$$

Der Definitionsbereich von T' ist also der Wertebereich von B. Wegen $|T'y| = |y|$ kann man T' stetig in die abgeschlossene Hülle $\mathfrak{N}$ des Wertebereichs von B fortsetzen;

der so fortgesetzte Operator heiße T_0. Es gilt also

$$T_0 \lim_{n\to\infty} y_n = \lim_{n\to\infty} T' y_n$$

für y_n im Wertebereich von B, $\lim y_n \in \mathfrak{R}$.

Nach Definition von T_0 ist

$$T_0 B = N - A,$$

nach Definition von A ist aber

$$N - A = -(N^* - A).$$

Aus beidem zusammen folgt

$$N = A + T_0 B, \quad N^* = A - T_0 B.$$

Wegen

$$((N-A)x,\ (N-A)y) = (Bx, By)$$

ist T' und damit auch T_0 ein isometrischer Operator. Um zu beweisen, daß $\mathfrak{R}$ durch T_0 unitär in sich transformiert wird, haben wir nur zu zeigen, daß $\mathfrak{R}$ der Wertebereich von T_0 ist. — Der Wertebereich von T' war der von $N - A$, der Wertebereich von T_0 ist darum der vom Wertebereich von $N - A$ erzeugte Unterraum (T_0 ist ja isometrisch); dieser ist [43]) das orthogonale Komplement des Unterraums aller x mit $(N-A)^* x = 0$ oder wegen $(N-A)^* = -(N-A)$ das orthogonale Komplement des Unterraums aller x mit $(N-A)x = 0$. Weil aber $(N-A)x = 0$ und $Bx = 0$ gleichbedeutend sind, ist der Wertebereich von T_0 auch das orthogonale Komplement des Unterraums der x mit $Bx = 0$. Damit ist schon bewiesen, daß der Wertebereich von T_0 gleich $\mathfrak{R}$ ist, daß T_0 also $\mathfrak{R}$ unitär auf sich abbildet.

Aus

$$T_0 B = N - A$$

folgt

$$T_0 B^2 = (N-A)\,B = B(N-A) = B T_0 B,$$

d. h.

$$T_0 B y = B T_0 y$$

für alle y im Wertebereich von B, aus Stetigkeitsgründen für alle $y \in \mathfrak{R}$, d. h.

$$T_0 \mathfrak{v} B_{\mathfrak{R}} \quad \text{in } \mathfrak{R}.$$

Nun existiert $B_{\mathfrak{R}}^{-1}$. Denn ist $z \in \mathfrak{R}$ und $B_{\mathfrak{R}} z = Bz = 0$, so liegt z nach Definition von $\mathfrak{R}$ im orthogonalen Komplement von $\mathfrak{R}$; weil auch $z \in \mathfrak{R}$ sein sollte, muß $z = 0$ sein. Aus $N - A = T_0 B$ folgt daher

$$N_{\mathfrak{R}} - A_{\mathfrak{R}} = T_0 B_{\mathfrak{R}} = B_{\mathfrak{R}} T_0,$$
$$B_{\mathfrak{R}}^{-1}(N_{\mathfrak{R}} - A_{\mathfrak{R}}) = T_0.$$

Ist nun C irgendein beschränkter Operator mit $C \mathfrak{v} N$, $C \mathfrak{v} N^*$, so gilt, wie wir schon wissen, auch $C \mathfrak{v} A$, $C \mathfrak{v} B$, und $\mathfrak{R}$ reduziert C; nun können wir auch noch schließen

$$C_{\mathfrak{R}} \mathfrak{v} B_{\mathfrak{R}}^{-1}(N_{\mathfrak{R}} - A_{\mathfrak{R}}) = T_0.$$

Das gilt insbesondere für $C = N$ und für $C = N^*$.

Damit sind alle Aussagen des Hauptsatzes bestätigt bis auf diese: T_0 soll in $\mathfrak{R}$ Imaginäroperator sein. Wir wissen bisher nur, daß T_0 in $\mathfrak{R}$ unitär ist. Nun ist aber der Wertebereich von $B_{\mathfrak{R}}^2$ in $\mathfrak{R}$ dicht, denn aus $z \in \mathfrak{R}$, $z \perp B^2 y$ für alle $y \in \mathfrak{R}$ folgt $z \perp B^3 x$ für alle $x \in \mathfrak{R}$, $B^3 z \perp x$ für alle $x \in \mathfrak{R}$ (weil B hermitesch ist), $B_{\mathfrak{R}}^3 z = 0$; weil aber $B_{\mathfrak{R}}^{-1}$ existiert, ist das nur für $z = 0$ möglich. Aus der Gleichung

$$T_0^2 B_{\mathfrak{R}}^2 = T_0(N_{\mathfrak{R}} - A_{\mathfrak{R}}) B_{\mathfrak{R}} = (N_{\mathfrak{R}} - A_{\mathfrak{R}}) T_0 B_{\mathfrak{R}} = (N_{\mathfrak{R}} - A_{\mathfrak{R}})^2$$
$$= -(N_{\mathfrak{R}} - A_{\mathfrak{R}})^*(N_{\mathfrak{R}} - A_{\mathfrak{R}}) = -B_{\mathfrak{R}}^2$$

folgt deshalb

$$T_0^2 x = -x$$

für alle x im Wertebereich von $B^2_{\mathfrak{R}}$, also auch für alle $x \in \mathfrak{R}$, d. h.

$$T_0^2 = -E_{\mathfrak{R}}.$$

Damit ist auch gezeigt, daß T_0 in $\mathfrak{R}$ Imaginäroperator ist, und der Hauptsatz über normale Operatoren ist für den Fall beschränkter normaler Operatoren bewiesen.

3. Wir stellen nun drei Sätze auf, die, wie sofort zu sehen ist, für jeden normalen Operator gelten, für den der Hauptsatz richtig ist, insbesondere also für jeden beschränkten normalen Operator. In § 14 werden wir sie für beliebige normale Operatoren beweisen und daraus dann rückwärts die Allgemeingültigkeit des Hauptsatzes erschließen.

I. *Ist N ein normaler Operator, so reduziert der von allen x mit $Nx = N^*x$ erzeugte Unterraum N und jeden beschränkten mit N und N^* vertauschbaren Operator.*

Beweis. Wegen

$$N = A + T_0 B, \qquad N^* = A - T_0 B$$

ist $Nx = N^*x$ mit $T_0 Bx = 0$ gleichwertig; T_0 ist aber in $\mathfrak{R}$ Imaginäroperator, darum folgt $Bx = 0$, x liegt im orthogonalen Komplement von $\mathfrak{R}$; $\mathfrak{R}$ und darum auch $\mathfrak{R} \ominus \mathfrak{R}$ reduziert aber, wie im Hauptsatz steht, N und jeden beschränkten mit N und N^* vertauschbaren Operator.

II. *Zu jedem normalen Operator gibt es einen Projektor P_- (er heiße in Analogie zu § 7 0-Projektor von N) mit folgenden Eigenschaften:*

1. *Aus $C \mathfrak{v} N$, $C \mathfrak{v} N^*$ folgt $C \mathfrak{v} P_-$.*
2. *$P_- \mathfrak{v} N$, $P_- \mathfrak{v} N^*$.*
3. *$((N + N^*)P_- x, x) \leqq 0$, wo $(N + N^*) P_- x$ sinnvoll ist.*
4. *$((N + N^*)(E - P_-)x, x) \geqq 0$, wo $(N + N^*)(E - P_-)x$ sinnvoll ist.*
5. *Aus $Nx + N^*x = 0$ folgt $P_- x = 0$.*

Beweis. Für P_- nimmt man den 0-Projektor von A. Die Eigenschaften 1. und 2. folgen dann aus c) und b) des Hauptsatzes, in bezug auf 3., 4. und 5. beachte man nur, daß (wegen d)) gilt

$$N + N^* \leqq 2A.$$

Um III formulieren zu können, machen wir eine Vorbemerkung: Ist T Imaginäroperator, so folgt aus $T \mathfrak{v} R$, daß sogar $TR = RT$ ist. Denn es gilt

$$TR \leqq RT = -T^2 RT \leqq -TRT^2 = TR,$$

also muß hier überall das Gleichheitszeichen stehen.

Hieraus folgt: Ist N normal, T Imaginäroperator, $T \mathfrak{v} N$, $T \mathfrak{v} N^*$, so ist auch TN normal mit $(TN)^* = -TN^*$. Denn:

$$(TN)^* = N^* T^* = -N^* T = -TN^*,$$
$$TN(TN)^* = -TNTN^* = -T^2 NN^* = NN^*,$$
$$(TN)^* TN = -TN^* TN = -T^2 N^* N = N^* N = NN^*.$$

III. *Zu jedem normalen Operator N mit der Eigenschaft, daß $Nx = N^*x$ nur für $x = 0$ gilt, gibt es einen Imaginäroperator T_0, der mit N, N^* und allen mit N und N^* vertauschbaren beschränkten Operatoren vertauschbar ist, so daß der 0-Projektor des normalen Operators $T_0^{-1} N$ gleich 0 wird.*

Beweis. Die Voraussetzung, daß $Nx = N^*x$ nur für $x = 0$ gilt, besagt, wie aus der im Anschluß an I gemachten Bemerkung ersichtlich ist, genau $\mathfrak{R} = \mathfrak{R}$; wir weisen die Eigenschaften für das T_0 des Hauptsatzes nach, das ja jetzt in ganz $\mathfrak{R}$ Imaginäroperator ist. Die Vertauschbarkeitsaussage für dies T_0 steht schon im Hauptsatz, es

ist nur zu zeigen, daß 0 im Sinne von II 0-Projektor von $T_0^{-1}N$ ist. Und dazu genügt es wieder,

$$((T_0^{-1}N + (T_0^{-1}N)^*)x, x) \geqq 0$$

nachzuweisen. Nun ist nach d)

$$T_0^{-1}N = T_0^{-1}A + B,$$
$$(T_0^{-1}N)^* = -T_0^{-1}N^* = -T_0^{-1}A + B,$$
$$T_0^{-1}N + (T_0^{-1}N)^* < 2B;$$

B war aber nichtnegativ definit.

4. *Der* 0*-Projektor eines normalen Operators N ist durch N eindeutig bestimmt.* Das zeigt man analog wie beim Fall eines selbstadjungierten Operators [45]) so: Sind P_- und Q_- zwei 0-Projektoren von N, so ist

$$P_- - Q_- = P_-(E - Q_-) - (E - P_-)Q_-;$$

wegen 1. und 2. gilt $P_- \mathfrak{v} Q_-$, rechts steht also die Differenz zweier Projektoren. Für alle $x \in P_-(E - Q_-)\mathfrak{R}$ gilt $P_-x = x$ und $(E - Q_-)x = x$, also nach 3. und 4. sowohl $((N + N^*)x, x) \leqq 0$ wie $((N + N^*)x, x) \geqq 0$, also $((N + N^*)x, x) = 0$; weil $N + N^*$ hermitesch ist [46]), folgt in bekannter Weise $(N + N^*)P_-(E - Q_-)\mathfrak{R} = 0$, wegen 5. $P_-P_-(E - Q_-)\mathfrak{R} = 0$, $P_-(E - Q_-) = 0$. Analog zeigt man $(E - P_-)Q_- = 0$.

Auch das T_0 von III *ist durch N eindeutig bestimmt.*

Beweis. Aus $Nx = N^*x$ folge $x = 0$, und mit T_0 habe auch der Imaginäroperator T_1 die obigen Eigenschaften. Dann sind T_0 und T_1 vertauschbar, und

$$\frac{E - T_0T_1}{2}$$

ist ein Projektor; setzt man

$$\frac{E - T_0T_1}{2}\mathfrak{R} = \mathfrak{M}, \quad \mathfrak{R} \ominus \mathfrak{M} = \mathfrak{N},$$

so ist

$$T_0x = T_1x \qquad \text{für } x \in \mathfrak{M},$$
$$T_0x = -T_1x \qquad \text{für } x \in \mathfrak{N} \text{ [47]}).$$

Wir haben zu zeigen, daß $\mathfrak{N} = 0$ ist. Für $x \in \mathfrak{N}$ ist aber

$$((T_0^{-1}N + (T_0^{-1}N)^*)x, x) \geqq 0 \quad \text{und} \quad ((T_1^{-1}N + (T_1^{-1}N)^*)x, x) \geqq 0,$$

wenn diese Ausdrücke existieren; aus beidem zusammen folgt aber wegen $x \in \mathfrak{N}$

$$(T_0^{-1}N + (T_0^{-1}N)^*)x = 0$$

analog zu einem oben gebrauchten Schluß. Weil aber

$$T_0^{-1}N + (T_0^{-1}N)^* = T_0^{-1}(N - N^*)$$

ist, folgt

$$(N - N^*)x = 0;$$

nach der Voraussetzung über N folgt daraus $x = 0$. Diese x liegen, weil $T_0^{-1}N + (T_0^{-1}N)^*$ hermitesch ist, in $\mathfrak{N}$ dicht, daher ist in der Tat

$$\mathfrak{N} = 0.$$

---

[45]) Rellich [3] S. 7.

[46]) Ist N normal, so ist $N + N^*$ hermitesch. Denn $((N + N^*)x, y) = (x, (N + N^*)y)$ ist trivial; der Wertebereich von $(N^*N + E)^{-1} = (NN^* + E)^{-1}$ ist aber in $\mathfrak{R}$ dicht, und in ihm sind N und N^* überall erklärt, darum ist der Definitionsbereich von $N + N^*$ in $\mathfrak{R}$ dicht. Dasselbe gilt natürlich in jedem N (und daher auch N^* und $N + N^*$) reduzierenden Unterraum.

[47]) Beweis analog zu § 9, **4** (dort war $T_0 = iE$, $T_1 = T$ gesetzt).

§ 14. Beweis des Hauptsatzes.

1. Wir beweisen zunächst, daß für einen normalen Operator N, für den der Hauptsatz gilt, A, B, $\mathfrak{K}$ und T_0 durch N eindeutig bestimmt sind. Zunächst ist $\mathfrak{K}$ als orthogonales Komplement des von den x mit $Nx = N^*x$ erzeugten Unterraums eindeutig durch N festgelegt. Ferner ist der 0-Projektor von $A - \lambda E$ ($\lambda \in R$) auch 0-Projektor des normalen Operators $N - \lambda E$, wie im Anschluß an II gezeigt wurde (die dortige Beschränkung auf $\lambda = 0$ ist unerheblich), als solcher ist er durch N eindeutig bestimmt. Die Spektralschar von A und damit A selbst ist also eindeutig festgelegt. Nun benutzen wir die Reduktionsinvarianz des Hauptsatzes. Damit ist folgendes gemeint: Ist $\mathfrak{M}$ irgendein Unterraum, der N reduziert, so kann man einfach die Definitionsbereiche von N, N^*, A, B, T_0 auf ihre Durchschnitte mit $\mathfrak{M}$ verengen und auch $\mathfrak{K}$ durch $\mathfrak{K} \cap \mathfrak{M}$ ersetzen, dann hat man den Hauptsatz für das so eingeengte $N_{\mathfrak{M}}$ dastehen. Ein Beweis dieser einfachen Tatsache ist nicht nötig. Wenn $\mathfrak{M}$ außerdem jeden mit N und N^* vertauschbaren Operator reduziert, so folgt sogar aus der Gültigkeit des Hauptsatzes für $N_{\mathfrak{M}}$ und für $N_{\mathfrak{R} \ominus \mathfrak{M}}$ auch wieder seine Gültigkeit für N selbst. Wir werden das später beim Beweis des Hauptsatzes noch anwenden. Schon jetzt aber sehen wir: Weil T_0 nur in $\mathfrak{K}$ erklärt ist und weil $B(\mathfrak{R} \ominus \mathfrak{K}) = 0$ gilt, genügt es, die eindeutige Bestimmtheit von T_0 und B in $\mathfrak{K}$ zu zeigen. Nach dem oben ausgesprochenen Prinzip kann man sich, weil $\mathfrak{K}$ N reduziert, dabei überhaupt auf die Betrachtung von N in $\mathfrak{K}$ beschränken, d. h. man kann annehmen, daß $\mathfrak{K}$ der ganze Raum sei: $\mathfrak{K} = \mathfrak{R}$. Dann sind aber die Voraussetzungen von III erfüllt. Wie schon dort bewiesen wurde, ist T_0 dann der Imaginäroperator, dessen Existenz in III behauptet wird, als solcher ist er eindeutig bestimmt. Schließlich ist ohne Mühe analog II zu sehen, daß für $\lambda \in R$ der 0-Projektor von $B - \lambda E$ zugleich auch 0-Projektor von $T_0^{-1} N - \lambda E$ ist, darum sind alle Spektralprojektoren von B und damit auch B durch N eindeutig bestimmt.

2. Dieser Beweis zeigt schon, wie wir unter Voraussetzung der uneingeschränkten Gültigkeit von I, II und III den Hauptsatz allgemein beweisen können. Sei also N irgendein normaler Operator. Dann reduziert nach I der von den x mit $Nx = N^*x$ erzeugte Unterraum $\mathfrak{M}$ den Operator N und alle mit N und N^* vertauschbaren beschränkten Operatoren. Nach dem obigen Reduktionsprinzip genügt es also, den Hauptsatz für $N_{\mathfrak{M}}$ und, $\mathfrak{R} \ominus \mathfrak{M} = \mathfrak{K}$ gesetzt, für $N_{\mathfrak{K}}$ zu beweisen. Mit anderen Worten, es genügt den Hauptsatz in folgenden beiden Extremfällen zu beweisen:

a) Die x mit $Nx = N^*x$ liegen im Raum dicht.

b) Aus $Nx = N^*x$ folgt $x = 0$.

Wir werden diesen Nachweis nun unter Verwendung von II und III führen.

a) Die x mit $Nx = N^*x$ mögen in $\mathfrak{R}$ dicht liegen. Dann sei P_λ der 0-Projektor von $N - \lambda E$. Ganz analog zu Rieß [1] S. 45—51 sieht man: die P_λ sind eine Spektralschar, und bezeichnet man den Operator, der den x mit $Nx = N^*x$ dies Nx, den übrigen x nichts zuordnet, mit A, so ist (A abgeschlossen und in einer in $\mathfrak{R}$ dichten Menge definiert und deshalb)

$$A = \int_{-\infty}^{+\infty} \lambda \, dP_\lambda .$$

Aus $N \geqq A$ und $N^* \geqq A$ folgt nun $N \leqq A^* = A$, $N = A$. Man kann also das A des Hauptsatzes gleich unserem $A = N$ setzen; man wird dann $B = 0$, $\mathfrak{K} = 0$ zu setzen haben, T_0 braucht nicht erst definiert zu werden ($T_0 0 = 0$). Man sieht ohne weiteres, daß sämtliche Behauptungen a)—d) des Hauptsatzes richtig sind. In diesem Extremfall hat sich also N als selbstadjungiert ergeben.

b) Nun folge aus $Nx = N^*x$, daß $x = 0$. Dann setzen wir $\mathfrak{K} = \mathfrak{R}$. Wegen III gibt es einen Imaginäroperator T_0, der mit N und allen beschränkten mit N und N^* vertauschbaren Operatoren vertauschbar ist, so daß der 0-Projektor von $T_0^{-1}N$ verschwindet, d. h. daß stets

$$((T_0^{-1}N + (T_0^{-1}N)^*)\,x,\, x) \geqq 0$$

gilt. Wir bezeichnen für reelle λ' und λ'' mit $P_{\lambda'}$ den 0-Projektor von $N - \lambda' E$, mit $Q_{\lambda''}$ den 0-Projektor von $T_0^{-1}N - \lambda'' E$. Wie bei Rieß [1] S. 45—51 sieht man: Die $P_{\lambda'}$ und die $Q_{\lambda''}$ sind je eine Spektralschar, sie sind mit N und N^* und mit allen mit N und N^* vertauschbaren beschränkten Operatoren vertauschbar, für $\lambda'' \leqq 0$ ist $Q_{\lambda''} = 0$. Es sei

$$A = \int_{-\infty}^{+\infty} \lambda'\, dP_{\lambda'}, \quad B = \int_{0}^{\infty} \lambda''\, dQ_{\lambda''}.$$

Dann sind mit diesen A, B, $\mathfrak{K}$, T_0 alle Aussagen des Hauptsatzes erfüllt bis auf d). (Daß $\mathfrak{K}$ wirklich das orthogonale Komplement des Unterraums aller x mit $Bx = 0$ ist, folgt so: Weil $T_0^{-1}N + (T_0^{-1}N)^*$ hermitesch ist und wegen $Q_0 = 0$ ist $(\lim_{\lambda'' \to +0} Q_{\lambda''})\mathfrak{R}$ der von allen x mit $(T_0^{-1}N + (T_0^{-1}N)^*)\,x = 0$ erzeugte Unterraum, also (vgl. § 13, **4**) der von den x mit $Nx = N^*x$ erzeugte Unterraum, also 0; daher $\lim_{\lambda'' \to +\infty} Q_{\lambda''} = 0$, d. h. auch aus $Bx = 0$ folgt $x = 0$.)

Ist nun $\lambda' < \mu'$ und $\lambda'' < \mu''$, so setze man

$$\Delta = (P_{\mu'} - P_{\lambda'})\,(Q_{\mu''} - Q_{\lambda''});$$

ist dann $x \in \Delta\mathfrak{R}$ und sind Nx und N^*x sinnvoll, so ist

$$\left|\frac{N + N^*}{2}\,x - \lambda' x\right| \leqq (\mu' - \lambda')\,|x| \quad \text{und} \quad \left|T_0^{-1}\left(\frac{N - N^*}{2}\right)x - \lambda'' x\right| \leqq (\mu'' - \lambda'')\,|x|,$$

mithin $$|Nx - \lambda' x - \lambda'' T_0 x| \leqq (\mu' - \lambda' + \mu'' - \lambda'')\,|x|$$
und $$|N^*x - \lambda' x + \lambda'' T_0 x| \leqq (\mu' - \lambda' + \mu'' - \lambda'')\,|x|.$$

Daraus folgt, daß ganz $\Delta\mathfrak{R}$ zum Definitionsbereich von N und zum Definitionsbereich von N^* gehört, und daß Nx und N^*x dann und nur dann existieren, wenn

$$\int_{-\infty}^{+\infty}\int_{0}^{\infty} (\lambda'^2 + \lambda''^2)\,(dQ_{\lambda''}\,dP_{\lambda'}\,x,\, x)$$

existiert, und daß dann

$$Nx = \int_{-\infty}^{+\infty}\int_{0}^{\infty} (\lambda' + \lambda'' T_0)\,dQ_{\lambda''}\,dP_{\lambda'}\,x, \qquad N^*x = \int_{-\infty}^{+\infty}\int_{0}^{\infty} (\lambda' - \lambda'' T_0)\,dQ_{\lambda''}\,dP_{\lambda'}\,x$$

ist. Auf Grund der bekannten Spektralformeln für Ax und Bx sieht man, daß sowohl Nx wie N^*x dann und nur dann existiert, wenn Ax und Bx existieren, und daß dann

$$Nx = Ax + T_0 Bx, \qquad N^*x = Ax - T_0 Bx$$

ist. Die Einzelheiten sind wieder analog zu Rieß [1].

3. Auf eine Verallgemeinerungsmöglichkeit sei kurz hingewiesen. Es könnte sein, daß aus $Nx = N^*x$ nicht notwendig $x = 0$ folgt, daß aber trotzdem ein mit N (und N^*) vertauschbarer Imaginäroperator T bekannt ist, für den auch nicht notwendig

$$((T^{-1}N + (T^{-1}N)^*)\,x,\, x) \geqq 0$$

zu gelten braucht. Dann kann man wie eben eine Spektralzerlegung

$$N = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} (\lambda' + \lambda'' T)\,dQ_{\lambda''}\,dP_{\lambda'}, \qquad N^* = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} (\lambda' - \lambda'' T)\,dQ_{\lambda''}\,dP_{\lambda'}$$

gewinnen. Die $P_{\lambda'}$ und die $Q_{\lambda''}$ werden mit N, N^* und T und allen mit N, N^* und T vertauschbaren beschränkten Operatoren vertauschbar sein. Man kann auch wieder

$$A = \int_{-\infty}^{+\infty} \lambda' dP_{\lambda'}, \qquad B = \int_{-\infty}^{+\infty} \lambda'' dQ_{\lambda''}$$

setzen und ein Analogon des Hauptsatzes aufstellen, das insofern einfacher wird, als die Schwierigkeiten mit $\mathfrak{R}$ wegfallen und T schon von vornherein gegeben ist. Dafür weiß man eben nicht, ob es ein solches T überhaupt gibt, wenn man nicht schon eine Spektralzerlegung von N kennt.

Insbesondere kann man im Hilbertschen Raum $T = iE$ setzen und kommt so zu der bekannten Spektralzerlegung normaler Operatoren im Hilbertschen Raum [41]) zurück.

4. Nach dem Vorhergehenden wird der Hauptsatz über normale Operatoren bewiesen sein, wenn die in § 13, **3** formulierten Behauptungen I, II, III, deren Gültigkeit bisher nur für beschränkte Operatoren feststeht, für beliebige normale Operatoren bewiesen sein werden. Dazu sind einige Vorbereitungen nötig.

Wie immer seien F und V durch

$$F\{x, y\} = \{x, 0\}, \qquad V\{x, y\} = \{y, -x\}$$

als Projektor bzw. Imaginäroperator in $\mathfrak{R}^2$ erklärt. N sei ein normaler Operator, B der zu $\mathfrak{B}_N$ gehörende Projektor. Wir wollen B explizit ausrechnen. Dazu sei

$$H = (N^*N + E)^{-1} = (NN^* + E)^{-1}.$$

Nach § 3, **4** ist das ein beschränkter selbstadjungierter Operator. Wegen

$\{x, 0\} = \{Hx, NHx\} + \{N^*NHx, -NHx\}, \{0, y\} = \{N^*Hy, NN^*Hy\} - \{N^*Hy, -Hy\}$

ist

$$B\{x, y\} = \{Hx + N^*Hy, NHx + NN^*Hy\},$$

denn $\mathfrak{B}_N$ war ja die Menge der sinnvollen $\{z, Nz\}$, $\mathfrak{R}^2 \ominus \mathfrak{B}_N$ die Menge der sinnvollen $\{N^*\zeta, -\zeta\}$. Bildet man nun

$$D = BFVB - (E - B)FV(E - B), \tag{1}$$

so ist unter Berücksichtigung von $(E - B)\{x, y\} = \{x - Hx - N^*Hy, -NHx + Hy\}$:

$$\begin{aligned} D\{x, y\} &= \{H(NHx + NN^*Hy), NH(NHx + NN^*Hy)\} \\ &\quad - \{-NHx + Hy - H(-NHx + Hy), -NH(-NHx + Hy)\} \\ &= \{NHx, NHy\}, \\ D &= \overline{NH}. \end{aligned}$$

Darum nach § 4, **3**

$$F \mathfrak{v} D, \; V \mathfrak{v} D. \tag{2}$$

Trivialerweise gilt auch

$$B \mathfrak{v} D. \tag{3}$$

Schließlich ist

$$D^* = -BVFB + (E - B)VF(E - B) \mathfrak{v} D. \tag{4}$$

Bei Beachtung von

$$FV + VF = V$$

(vgl. § 7, **3**) folgt daraus

$$D - D^* = BVB - (E - B)V(E - B). \tag{5}$$

D ist also ein beschränkter normaler Operator in $\mathfrak{R}^2$. Ferner gilt

$$C \mathfrak{v} N, N^* \text{ genau wenn } \bar{C} \mathfrak{v} B. \tag{6}$$

Denn $C \mathfrak{v} N$ und $C \mathfrak{v} N^*$ gelten dann nur dann, wenn $C \mathfrak{v} N$ und $C^* \mathfrak{v} N$ (§ 4, **1**), also dann

und nur dann, wenn $\bar{C}\mathfrak{B}_N \leq \mathfrak{B}_N$ und $\bar{C}^*\mathfrak{B}_N \leq \mathfrak{B}_N$ [48]), nach dem Zusatz von § 4, 2 heißt das genau $\bar{C}\mathfrak{v}B$.

Weil für alle beschränkten C

$$\bar{C}\,\mathfrak{v}F,\ V$$

gilt, folgt:

(7) Aus $C\mathfrak{v}N,\ N^*$ folgt $\bar{C}\mathfrak{v}D,\ D^*$.

Mit Hilfe von (1) und (4) rechnet man schließlich leicht nach:

$$(D\{z, Nz\}, \{z, Nz\}) = (Nz, z), \tag{8}$$

$$(D^*\{z, Nz\}, \{z, Nz\}) = (z, Nz). \tag{9}$$

Weil D normal und beschränkt ist, gelten die Sätze I, II, III für D. Wir werden sie so lange umformen, bis sie für N dastehen.

Der Definitionsbereich von N heiße $\mathfrak{D}$.

5. Weil I für D gilt, ist der Projektor, der zum Unterraum aller $\{x, y\}$ mit

$$D\{x, y\} = D^*\{x, y\}$$

gehört, mit D und allen mit D und D^* vertauschbaren Operatoren vertauschbar. Insbesondere ist er mit F und V vertauschbar, darum kann er (§ 4, 3) gleich in der Form $\bar{P}$ geschrieben werden. Ferner ist $\bar{P}$ mit B vertauschbar, d. h. nach (6)

$$P\mathfrak{v}N,\ N^*.$$

Und aus $C\mathfrak{v}N,\ N^*$ folgt nach (7) $\bar{C}\mathfrak{v}D,\ D^*$, daraus $\bar{C}\mathfrak{v}\bar{P},\ C\mathfrak{v}P$. Jetzt fehlt nur noch der Nachweis, daß $P\mathfrak{R}$ genau der von den z mit $Nz = N^*z$ erzeugte Unterraum ist.

$\mathfrak{D}$ liegt in $\mathfrak{R}$ dicht und $P\mathfrak{R}$ reduziert N, darum ist $\mathfrak{D} \cap P\mathfrak{R}$ in $P\mathfrak{R}$ dicht (vgl. § 4, 2). Es genügt also, zu zeigen, daß $z \in \mathfrak{D} \cap P\mathfrak{R}$ und $Nz = N^*z$ gleichwertig sind. Wegen $P\mathfrak{v}N$ besagt aber $z \in \mathfrak{D} \cap P\mathfrak{R}$ genau $\{z, Nz\} \in \bar{P}\mathfrak{R}^2$, d. h.

$$(D - D^*)\{z, Nz\} = 0$$

oder wegen (5)

$$\begin{aligned} &B\{Nz, -z\} = 0,\\ &\{Nz, -z\} \in \mathfrak{R}^2 \ominus \mathfrak{B}_N = V\mathfrak{B}_{N^*},\\ &Nz = N^*z. \end{aligned}$$

Damit ist I schon bewiesen.

6. Weil II für D gilt, gibt es einen Projektor — wir können ihn wie oben gleich in der Form $\overline{P_-}$ schreiben — mit den Eigenschaften:

1. Aus $G\mathfrak{v}D$ und $G\mathfrak{v}D^*$ folgt $G\mathfrak{v}\overline{P_-}$.
2. $\overline{P_-}\mathfrak{v}D,\ \overline{P_-}\mathfrak{v}D^*$.
3. $((D + D^*)\,\overline{P_-}x, x) \leqq 0$
4. $((D + D^*)\,(\bar{E} - \overline{P_-})\,x, x) \geqq 0$ $\Big\}\ (x \in \mathfrak{R}^2)$.
5. Aus $(D + D^*)x = 0$ folgt $\overline{P_-}x = 0$

Wir beweisen, daß P_- die analogen Eigenschaften in bezug auf N hat.

1. Aus $C\mathfrak{v}N,\ N^*$ folgt nach (7) $\bar{C}\mathfrak{v}D,\ D^*$, nach 1. $\bar{C}\mathfrak{v}\overline{P_-},\ C\mathfrak{v}P_-$.
2. Aus $B\mathfrak{v}D,\ D^*$ folgt nach 1. $B\mathfrak{v}\overline{P_-}$, nach (6) $P_-\mathfrak{v}N,\ N^*$.
3. Aus $P_-z = z,\ z \in \mathfrak{D}$ folgt

$$\overline{P_-}\{z, Nz\} = \{z, Nz\},$$

nach 3.

$$((D + D^*)\{z, Nz\}, \{z, Nz\}) \leqq 0,$$

---

[48]) Nach § 4, 3. Man beachte dabei $\bar{C}^* = \overline{C^*}$ (§ 3, 4).

nach (8) und (9)

$$(Nz, z) + (z, Nz) \leqq 0,$$

deshalb gilt allgemein

$$((N + N^*) P_- z, z) \leqq 0.$$

4. Genau so beweist man

$$((N + N^*) (E - P_-) z, z) \geqq 0.$$

5. Wie man leicht nachrechnet, ist

$$(D + D^*) \{z, Nz\} = B \{Nz, z\},$$

aus $Nz + N^*z = 0$ folgt darum

$$(D + D^*) \{z, Nz\} = - B\{N^*z, -z\} = 0,$$

nach 5.

$$\overline{P_-}\{z, Nz\} = 0,$$
$$P_- z = 0.$$

Damit ist die Gültigkeit von II auch für N bewiesen.

7. Weil III für D gilt, gibt es in $\mathfrak{R}^2$ einen mit D, D^* und allen mit D und D^* vertauschbaren beschränkten Operatoren vertauschbaren Imaginäroperator — er kann wieder gleich $\overline{T}_0$ geschrieben werden — mit

$$(\overline{T}_0^{-1}(D - D^*) x, x) \geqq 0.$$

T_0 wird die in III behaupteten Eigenschaften in bezug auf N haben. Daß T_0 mit N, N^* und allen beschränkten mit N und N^* vertauschbaren Operatoren vertauschbar ist, folgt wie in § 14, **5** und **6**. Wegen (5) und $B \mathfrak{v} \overline{T}_0$ ist aber

$$0 \leqq (\overline{T}_0^{-1}(D - D^*) \{z, Nz\}, \{z, Nz\}) = (T_0^{-1} Nz, z) - (T_0^{-1} z, Nz) = (T_0^{-1}(N - N^*) z, z).$$

Auch III gilt also für beliebiges N.

Damit ist auch der Hauptsatz über normale Operatoren allgemein bewiesen.

Literaturverzeichnis.

Friedrichs 1: Spektraltheorie halbbeschränkter Operatoren usw., Math. Annalen **109** (1934).

Hausdorff 1: Zur Theorie der linearen metrischen Räume, Journal f. d. r. u. a. Math. **167** (1932).

Jordan 1: Über die Multiplikation quantenmechanischer Größen II, Zeitschrift f. Physik **87** (1934).

Löwig 1: Komplexe Euklidische Räume von beliebiger endlicher oder transfiniter Dimensionszahl, Acta litt. ac. sc. Szeged **7** (1934).

v. Neumann 1: Allgemeine Eigenwerttheorie Hermitescher Funktionaloperatoren, Math. Ann. **102** (1930).

— 2: Zur Algebra der Funktionaloperationen und Theorie der normalen Operatoren, Math. Ann. **102** (1930).

— 3: Über adjungierte Funktionaloperatoren, Annals of Math. **33** (1932).

Rellich 1: Spektraltheorie in nichtseparabeln Räumen, Math. Ann. **110** (1935).

— 2: Operatorentheorie
— 3: Spektraltheorie
} Seminarausarbeitungen, Göttingen 1933/34 und 1934.

Rieß 1: Über die linearen Transformationen des komplexen Hilbertschen Raumes, Acta litt. ac. sc. Szeged **5** (1930/32).

— 2: Zur Theorie des Hilbertschen Raumes, ebenda **7** (1934).

Stone 1: Linear Transformations in Hilbert Space usw., New York 1932.

v. d. Waerden 1: Moderne Algebra I, Berlin 1930.

Wecken 1: Zur Theorie linearer Operatoren, Math. Ann. **110** (1935).

Eingegangen 10. Juni 1935.

Längste konvexe Kurven, die einem gegebenen konvexen Polygon umschrieben sind.

Von *Anton E. Mayer* in Wien.

Die Überschrift weist auf eine Frage hin, die möglicherweise zu jenen zählt, die Jacob Steiner im Zusammenhang mit seinen elementargeometrischen Untersuchungen über Maxima und Minima beschäftigt haben [1]). Doch hat er die in Rede stehende Aufgabe allem Anschein nach nie ausdrücklich formuliert. Ich wurde auf sie durch eine von K. Menger veröffentlichte Mitteilung [2]) aufmerksam, die eine notwendige und hinreichende Bedingung dafür enthält, daß in der Menge der einem konvexen Polygon umschriebenen konvexen Kurven längste *existieren*.

Im folgenden wiederhole ich zunächst die Existenzbedingung und gelange hierauf zu einer *Konstruktion* dieser längsten Kurven, insofern nämlich, als ich endlich-viele Polygone bestimme, unter denen die gesuchten Kurven zu finden sind. (Mein Beweis hierfür ist auf der Existenz eines Maximums aufgebaut; er ließe sich aber auch so ausgestalten, daß mit ihm zugleich der Existenzbeweis erledigt würde.) Schließlich wird die Anzahl der in Betracht kommenden Polygone erörtert.

Ein konvexes Polygon K, als Flächenstück aufgefaßt, nicht als Streckenzug, sei durch seine Eckpunkte $\{p_i\}$ gegeben ($i \equiv 1, 2, \ldots, n \bmod n$). Das Polygon erfülle die Bedingung, daß je zwei aufeinanderfolgende Ecken eine Winkelsumme $> \pi$ haben (mithin ist $n > 4$). In diesem Falle schneidet die geradlinige Verlängerung der Seite $p_{i-1}p_i$ jenseits p_i die über p_{i+1} hinaus verlängerte Seite $p_{i+1}p_{i+2}$ in einem Punkte d_i. Die abgeschlossene Dreiecksfläche $p_i d_i p_{i+1}$ vermindert um die Strecke $p_i p_{i+1}$ werde mit D_i bezeichnet.

Wir betrachten das System $\mathfrak{L}$ der abgeschlossenen konvexen Mengen, die K umschrieben sind, worunter zu verstehen ist, daß der Rand jeder Menge L aus $\mathfrak{L}$ die Punktmenge $\{p_i\}$ enthält. Es ist

$$K \subseteq L \subseteq K + \sum_{i=1}^{n} D_i. \tag{1}$$

Die Mengen des Systems $\mathfrak{L}$ sind somit gleichmäßig beschränkt, ihr Umfang desgleichen. Daher [3]) gibt es in $\mathfrak{L}$ mindestens eine Menge M mit längstem Umfang [2]). (Dies trifft nicht zu, wenn die eingangs aufgestellte Bedingung für K außer acht gelassen wird.)

[1]) Vgl. J. Steiner, Gesammelte Werke **2**, Berlin 1882, S. 242, Schlußbemerkung.

[2]) K. Menger, Bemerkung über konvexe ebene Kurven, Ergebn. math. Kolloqu. **4** (1933), S. 14. Dort wird auch darauf hingewiesen, daß die fraglichen Kurven nur Polygone sein können.

[3]) Siehe den bekannten Konvergenzsatz für konvexe Mengen von W. Blaschke, Kreis und Kugel, Leipzig 1916, § 18.

Wir behaupten nun:

Die umfangsgrößte Menge M entsteht aus K durch Hinzufügen einiger Dreiecke aus der Folge $\{D_i\}$, also

$$M = K + \sum_{i=1}^{n} \varepsilon_i D_i \qquad (\varepsilon_i = 0 \text{ oder } 1)\,. \tag{2}$$

Da M existiert, wird der Beweis dieses Satzes erbracht sein, sobald gezeigt ist: zu jeder Menge L aus $\mathfrak{L}$, die *nicht* in der Form (2) dargestellt werden kann, gibt es eine Menge L^* aus $\mathfrak{L}$, die einen größeren Umfang als L hat.

Statt (1) schreiben wir nunmehr

$$\begin{cases} L = K + \sum_{i=1}^{n} T_i \\ T_i \leqq D_i \end{cases} \qquad \begin{cases} L^* = K + \sum_{i=1}^{n} T_i^* \\ T_i^* \leqq D_i \end{cases}$$

und nehmen an, es gäbe mindestens einen Index j, für den $0 < T_j < D_j$ ist. Jetzt sind zwei Fälle zu unterscheiden.

(Sonderfall) Wenn $T_{j-1} = T_{j+1} = 0$ und $T_j < D_j$, so setzen wir $T_j^* = D_j$, hingegen $T_i^* = T_i$ für $i \neq j$. Dann ist L^* konvex und K umschrieben. Weil $L^* > L$, besitzt L^* den längeren Umfang.

(Hauptfall) Gilt jedoch $0 < T_{j-1} < D_{j-1}$ und $0 < T_j < D_j$, so legen wir in den Punkten p_{j-1}, p_j, p_{j+1} an die Menge L die Stützgeraden S_{j-1}, S_j, S_{j+1}, die gemäß der Annahme von den Geraden $p_{j-1}p_j$ und p_jp_{j+1} verschieden sind, und bezeichnen mit q_{j-1}, q_{j+1} die Schnittpunkte $S_{j-1} \cdot S_j$ bzw. $S_j \cdot S_{j+1}$. Schließlich bilden wir die konvexe Hülle L' derjenigen Menge, die aus L und aus den Punkten q_{j-1}, q_{j+1} besteht. Nun zur entscheidenden Vergrößerung des Umfangs!

Der Kreis O berühre S_{j-1}, S_j, S_{j+1} in den Punkten s_{j-1}, s_j, s_{j+1} und zwar so, daß die Geraden S_{j-1}, S_{j+1} den Kreis O nicht von p_j trennen, während O und die Punkte p_{j-1}, p_{j+1} auf verschiedenen Seiten von S_j liegen (Fig. 1). Dann ist $q_{j-1}s_j = q_{j-1}s_{j-1}$

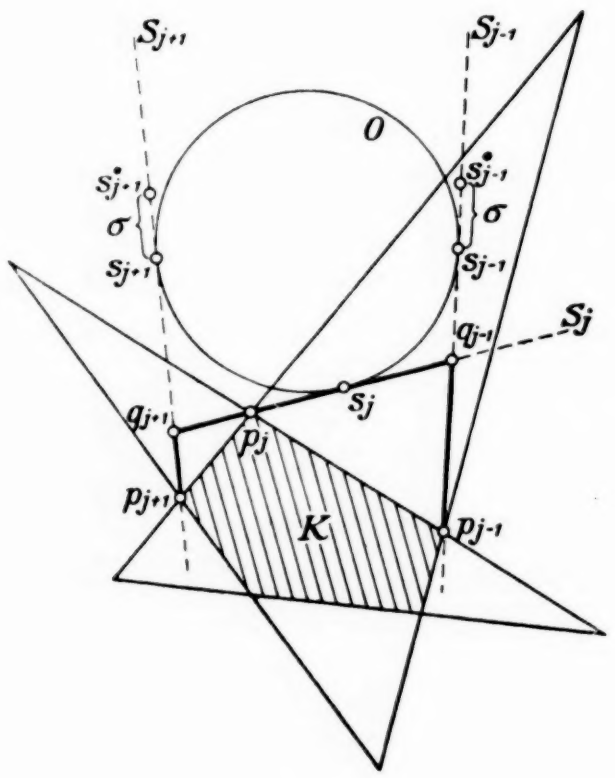

Fig. 1.

und $q_{j+1}s_j = q_{j+1}s_{j+1}$, somit die Länge des Streckenzuges $p_{j-1}q_{j-1}q_{j+1}p_{j+1}$ gleich $p_{j-1}s_{j-1} + p_{j+1}s_{j+1}$. Sind auf S_{j-1} und S_{j+1} noch die Punkte s^*_{j-1} bzw. s^*_{j+1} derart gelegen, daß

$$p_{j-1}s_{j-1} - p_{j-1}s_{j-1} = p_{j+1}s^*_{j+1} - p_{j+1}s_{j+1} = \sigma > 0$$

ist, so konstruieren wir den Kreis O^*, der S_{j-1} und S_{j+1} in s^*_{j-1} bzw. s^*_{j+1} berührt. Durch p_j geht eine Tangente an O^*, die sich beliebig wenig von S_j unterscheidet, wenn nur σ klein genug ist. Man kann daher bewirken, daß die erwähnte Tangente die Geraden S_{j-1}, S_{j+1} in Punkten q^*_{j-1}, q^*_{j+1} schneidet, die sich auf D_{j-1} bzw. D_j befinden, daß somit die Menge

$$L^* = L' - \underbrace{p_{j-1}q_{j-1}p_j - p_jq_{j+1}p_{j+1} + p_{j-1}q^*_{j-1}p_j + p_jq^*_{j+1}p_{j+1}}_{\text{Dreiecksflächen}}$$

wieder konvex und dem Polygon K umschrieben ist. Die Länge des Streckenzuges $p_{j-1}q^*_{j-1}q^*_{j+1}p_{j+1}$ ist $p_{j-1}s^*_{j-1} + p_{j+1}s^*_{j+1} = p_{j-1}s_{j-1} + p_{j+1}s_{j+1} + 2\sigma$. Demnach besitzt L^* einen längeren Umfang als L', also erst recht einen längeren Umfang als $L \leqq L'$, w. z. b. w.

Wir haben bisher dargetan, daß die Menge M größten Umfangs der Darstellung (2) fähig ist. Es fehlt noch an näheren Angaben über die zyklische Folge $\{\varepsilon_i\}$ der in (2) auftretenden Vorzeichen, welche umkehrbar-eindeutig der Menge M zugeordnet ist. Für $\{\varepsilon_i\}$ bestehen die Regeln:

I. Wenn $\varepsilon_j = 1$, so ist $\varepsilon_{j-1} = \varepsilon_{j+1} = 0$. Andernfalls wäre M nicht konvex.

II. Wenn $\varepsilon_{j-1} = \varepsilon_{j+1} = 0$, so ist $\varepsilon_j = 1$. Sonst könnte mittels des vorhin für den Sonderfall angegebenen Verfahrens der Umfang von M vergrößert werden.

Die Bedingungen I, II sind offensichtlich unabhängig und sie widersprechen einander nicht, da ja M existiert. Weitere Bedingungen, falls sie unter allen Umständen die Anzahl der I und II gemäßen Folgen $\{\varepsilon_i\}$ verminderten, wären unzulässig. Denn man kann leicht Beispiele angeben, in denen *alle* mit I und II verträglichen Folgen Mengen *gleichen* Umfangs ergeben. Für $n = 5$ (oder 7) enthalten nämlich sämtliche Folgen, die mit I und II im Einklang stehen, gleichviele Nullen (für andere Werte von $n > 4$ tritt dies nicht ein). Daher sind die aus einem regulären Fünfeck K (oder Siebeneck) nach (2), I und II konstruierten Figuren umfangsgleich.

Für $\{\varepsilon_i\}$ gibt es von vornherein 2^n verschiedene Anordnungen. Durch I und II scheiden viele dieser Möglichkeiten aus; übrig bleiben z. B.

	5,	5,	7,	10,	12,	17
für $n =$	5,	6,	7,	8,	9,	10.

Für größere Werte von n wird die unmittelbare Abzählung aller zyklischen Folgen, die I und II Genüge leisten, langwierig. Ihre Anzahl $g(n)$ läßt sich aber folgendermaßen berechnen.

Man setze formal

$$g(-1) = -1, \quad g(0) = 3, \quad g(1) = 0.$$

Aus diesen Anfangswerten ergibt sich — wir unterdrücken den Beweis — die Anzahl $g(n)$ mittels der Rekursionsformel

$$g(n) = g(n-2) + g(n-3).$$

Die zahlentheoretische Funktion $g(n)$ steht übrigens in naher Beziehung zu den Laméschen Zahlen vierter Ordnung, welche folgendermaßen definiert sind[4]):

$$L(n+1) = L(n) + L(n-4) \qquad (L(0) = L(1) = L(2) = L(3) = 0, \quad L(4) = 1).$$

So gilt beispielsweise die Relation

$$g(n) = 2\,L(n+2) + 3\,L(n-1) + L(n-4).$$

Die ganze vorangegangene Untersuchung und der zu Beginn formulierte Satz gelten völlig unverändert auch für die Kugelfläche und zwar dann, wenn das zugrunde zu legende konvexe sphärische Polygon aus dem Kugelmittelpunkt in ein ebenes konvexes Polygon projiziert werden kann, bei dem jedes Paar benachbarter Winkel eine Summe $> \pi$ ergibt. Freilich existiert zu *jedem* konvexen sphärischen Polygon eine längste umschriebene konvexe sphärische Kurve, auch in den Fällen $n = 2, 3, 4$.

[4]) Vgl. J. Hermes, Anzahl der Zerlegungen einer ganzen rationalen Zahl in Summanden, Math. Annalen **45** (1894), S. 371.

Rekurrente Zahlenfolgen, in denen $g(n)$ und $L(n)$ auf einfache Weise als Sonderfälle inbegriffen sind, betrachtete M. d'Ocagne, Théorie élémentaire des séries récurrentes, Nouv. annales math. (3) **3** (1884), S. 65. Die Zahlenfolge $g(n)$ selbst findet sich bei R. Perrin, Intermédiaire des math. **6** (1899), S. 76; E. Malo, ebenda **7** (1900), S. 280 u. 312.

Eingegangen 12. April 1935.

Untersuchungen in der Zahlentheorie der rationalen Quaternionenalgebren [1]).

Von *Martin Eichler* in Halle.

Einleitung.

Die Literatur über die rationalen Quaternionenalgebren, zu der auch die Brandtschen Arbeiten über die Kompositionstheorie der quaternären quadratischen Formen gerechnet werden müssen, kann in Anbetracht der Begrenztheit des Gebietes als sehr reichhaltig bezeichnet werden. Meine Arbeit hat die Aufgabe, einige bisher noch offen gebliebene Fragen zu beantworten.

Bezüglich der Grundbegriffe muß auf Arbeiten von Herrn Brandt [2]) verwiesen werden. Nachdem aus diesen Arbeiten die Wichtigkeit des Gruppoidbegriffes klar geworden ist, liegt die Frage nahe, wann ein beliebiger Modul überhaupt zu einem Gruppoid gehört, d. h. wann ein Modul umkehrbar ist. Die Antwort darauf gibt der erste Abschnitt dieser Arbeit in den Sätzen 2, 3, 4.

In der Dedekindschen Modultheorie spielt der Begriff des Komplements eine wichtige Rolle. Daß dies keineswegs nur im Kommutativen der Fall ist, geht schon aus der Kompositionstheorie der quadratischen Formen hervor, denn wie einem Modul eine Form als Normenform entspricht, so entspricht dem komplementären Modul die reziproke Form [3]). Die Dedekindschen Ansätze [4]) lassen sich leicht, wie es Herr Brandt kürzlich in einer Vorlesung getan hat, auf beliebige einfache hyperkomplexe Systeme übertragen. Damit sind die Eigenschaften des Komplements aber noch nicht erschöpft. Der Fuetersche Gedanke [5]) nämlich, zugleich mit einer Ordnung $\mathfrak{o} = [\ldots, \varrho_i, \ldots, \varrho_k, \ldots]$ die Zahlen $\varrho_i\varrho_k - \varrho_k\varrho_i$ zu betrachten, liefert eine direkte Konstruktion des Komplements einer Quaternionenordnung (§ 3). Jetzt beherrscht man die Eigenschaften des Komplements mit Leichtigkeit und gelangt auch zu einem vertieften Verständnis des wichtigen von

[1]) Diese Arbeit wurde von der Naturwissenschaftlichen Fakultät der Martin-Luther-Universität Halle-Wittenberg als Inauguraldissertation angenommen. Referent war Herr Professor Dr. H. Brandt.

[2]) H. Brandt, I. Zur allgemeinen Idealtheorie, Verh. d. Schweizer Naturf. Ges. Basel 1927, II. Teil, S. 86—88. Im folgenden stets zitiert als B. I. — II. Idealtheorie in einer Dedekindschen Algebra, Jahresbericht d. Deutschen Mathematikervereinigung **37** (1928), S. 5. Im folgenden zitiert als B. II. — III. Idealtheorie in Quaternionenalgebren, Math. Annalen **99** (1928), S. 1. Im folgenden zitiert als B. III. Vgl. zu den meisten Fußnoten die zusammenfassende Darstellung der Algebrentheorie von M. Deuring, Algebren, Ergebnisse der Mathematik und ihrer Grenzgebiete **4**, Berlin 1935.

[3]) Vgl. den zweiten Abschnitt.

[4]) R. Dedekind, I. Supplement XI zu Dirichlets Vorlesungen über Zahlentheorie, 4. Aufl. (1894). Besonders § 167. Im folgenden zitiert als D. I. — II. Über die Diskriminanten endlicher Körper, Abh. d. k. Ges. d. Wiss. zu Göttingen **29** (1882), S. 1. Im folgenden zitiert als D. II.

[5]) R. Fueter, Quaternionenringe, Comm. Math. Helv. **6** (1934), S. 199.

Herrn Brandt entdeckten Satzes, daß die Multiplikationszahlen einer Ordnung, die in reduzierter Basis vorliegt, aus ihrer Normenform berechnet werden können [6]).

Der § 3 schließt mit zwei Sätzen, welche alle Ordnungen mit umkehrbarem Komplement charakterisieren. Die Kenntnis des Satzes 5, sowie den Grundgedanken des zu Satz 6 mitgeteilten Beweises verdanke ich Herrn Brandt.

In § 4 wird der Führerbegriff eingeführt, und seine Grundeigenschaften werden entwickelt.

Von den bisher behandelten Problemen deutlich unterschieden ist dasjenige, alle Maximalordnungen zu finden, welche eine gegebene nichtmaximale Ordnung enthalten. Es geht auf Latimer [7]) zurück; weitergehend hat es Fueter bearbeitet [5]). Zu einer allgemeinen Lösung gelangt man aber erst durch Anwendung der Modul- und Idealtheorie, wie der dritte Abschnitt dieser Arbeit zeigen soll. Untersucht man die Quaternionenordnungen bezüglich Erweiterung zu umfassenderen Ordnungen, so stößt man auf zwei verschiedene Klassen: die eine umfaßt die Ordnungen, welche die Maximalordnung eines kommutativen quadratischen Unterkörpers enthalten; diese Ordnungen sollen *primitive* Ordnungen genannt werden. Die übrigen wollen wir *imprimitive* nennen, sie bilden die zweite Klasse. Primitive und imprimitive Ordnungen sind durch ein einfaches Kriterium (Satz 8) zu unterscheiden. Maximalordnungen und Durchschnitte von zwei solchen sind stets primitive Ordnungen (Satz 13).

Satz 9 reduziert nun die Frage nach den Maximalordnungen, welche eine gegebene imprimitive Ordnung enthalten, auf die entsprechende Frage für primitive Ordnungen. Aus dem Grunde dürfen die imprimitiven Ordnungen von den nun folgenden Untersuchungen ausgeschlossen werden. In § 6 wird das Restklassensystem $\mathfrak{S}_p$ einer primitiven Ordnung $\mathfrak{o}$ nach dem Modul $p\mathfrak{o}$ betrachtet, wobei p eine Primzahl ist. Schon in allgemeinen halbeinfachen Systemen konnte Herr Speiser [8]) aus der Struktur dieses Restklassensystems in gewissen Fällen auf die Existenz einer Erweiterungsordnung schließen. In dem hier vorliegenden einfachen Fall ist diese Betrachtungsweise erfolgreich.

Ist p eine die Diskriminante von $\mathfrak{o}$ teilende Primzahl, so teilt man die Ordnungen $\mathfrak{o}$ je nach der Struktur von $\mathfrak{S}_p$ in drei Typen ein, und kennzeichnet die einzelnen Fälle durch das Symbol $(\mathfrak{o}/p)$, welches die Werte $0, 1, -1$ annehmen kann. Es ist nicht mit dem von Hasse [9]) eingeführten Symbol (A/p) identisch; ist jedoch $\mathfrak{J}$ eine Maximalordnung einer Quaternionenalgebra A, so ist $(\mathfrak{J}/p) = -1$, sobald $(A/p) \equiv \frac{1}{2} \pmod 1$ ist, und $(\mathfrak{J}/p)$ nicht erklärt, wenn $(A/p) \equiv 0 \pmod 1$ ist. Das Symbol $(\mathfrak{o}/p)$ läßt sich auf das Legendresymbol zurückführen (Satz 10). Je nach seinem Wert stellt man ein verschiedenes Verhalten von $\mathfrak{o}$ in bezug auf Erweiterung fest (Satz 11, 12). Die Sätze 11, 12 gestatten es, alle Ordnungen zu berechnen, welche eine gegebene primitive Ordnung enthalten.

Die endgültige Lösung des Problems, alle Maximalordnungen zu charakterisieren, die eine gegebene primitive Ordnung enthalten, geschieht durch die Betrachtung der Ordnungen, welche Durchschnitte von Maximalordnungen sind (§ 7). Der wichtigste Satz dieses Paragraphen ist der Satz 13, der auch selbständiges Interesse beanspruchen

---

[6]) B. III, § 22. Dieser Satz wurde neu abgeleitet von R. Fueter, Zur Theorie der Brandtschen Quaternionenalgebren, Math. Annalen **110** (1935), S. 650, § 1.

[7]) C. G. Latimer, Arithmetics of generalized quaternion algebras, Amer. Journ. of Math. **48** (1926), S. 57.

[8]) A. Speiser, Idealtheorie in rationalen Algebren, Vierteljahrsschrift der Naturforschenden Gesellschaft Zürich **71** (1926) = XIII. Kapitel des Buches von L. E. Dickson, Algebren und ihre Zahlentheorie, Zürich 1927.

[9]) H. Hasse, Theory of cyclic algebras over an algebraic number field, Trans. Amer. Math. Soc. **34** (1932), S. 171.

darf. Er zeigt unter anderem, daß man das gestellte Problem nur für solche Ordnungen zu lösen hat, die Durchschnitt zweier Maximalordnungen sind; und da ist die Lösung sehr einfach (Satz 14, 15) und führt schließlich zu dem allgemeinen Satz 16.

Herrn Professor Dr. Brandt danke ich für die Anregung zur Beschäftigung mit diesem Thema, besonders auch für seine stete Hilfe und fördernde Kritik. Auch Herrn Dr. Grell bin ich für manchen Rat zu Dank verpflichtet.

I. Abschnitt.
Umkehrbarkeit von Quaternionenmoduln.

§ 1. Grundbegriffe.

1. Es werden beliebige Quaternionenalgebren über dem rationalen Zahlkörper betrachtet; das System der Matrizen zweiten Grades soll nicht ausgeschlossen werden. Die Voraussetzung über den Grundkörper beeinträchtigt die Allgemeinheit der Untersuchungen nur unwesentlich, da sie mühelos für einen beliebigen Zahlkörper als Grundkörper durchgeführt werden können.

Bezüglich der Bezeichnungen sollen folgende Festsetzungen getroffen werden: kleine lateinische Buchstaben bezeichnen rationale Zahlen, kleine griechische dagegen Quaternionen. Kleine Frakturbuchstaben bedeuten ausschließlich viergliedrige Moduln, mit Ausnahme der Maximalordnungen, die den Buchstaben $\mathfrak{J}$ erhalten sollen.

Die aus der *Hauptgleichung* des Systems genommene Spur und Norm wird

$$s(\alpha) = \alpha + \bar{\alpha}, \qquad n(\alpha) = \alpha \cdot \bar{\alpha}$$

geschrieben, wobei $\bar{\alpha}$ die zu α *konjugierte* Zahl bedeutet. Es ist stets $\overline{\alpha \cdot \beta} = \bar{\beta} \cdot \bar{\alpha}$. $\Delta(\alpha) = s(\alpha)^2 - 4n(\alpha)$ heißt die *Diskriminante von* α. Die aus zwei Zahlen α und β gebildete Zahl

$$\begin{aligned} n(\alpha, \beta) = s(\alpha)\, s(\beta) - s(\alpha\beta) &= n(\alpha + \beta) - n(\alpha) - n(\beta) = n(\beta, \alpha) \\ &= \alpha\bar{\beta} + \beta\bar{\alpha} = \bar{\alpha}\beta + \beta\alpha \end{aligned}$$

heißt die *Zwischennorm von* α *und* β.

Ersetzt man in einem Modul $\mathfrak{m}$ alle Zahlen durch die konjugierten, so erhält man wieder einen Modul; er heißt der zu $\mathfrak{m}$ *konjugierte Modul* und wird $\bar{\mathfrak{m}}$ geschrieben. Sind $\mathfrak{m}$ und $\mathfrak{n}$ zwei Moduln, so gilt $\overline{\mathfrak{m} \times \mathfrak{n}} = \bar{\mathfrak{n}} \times \bar{\mathfrak{m}}$; Ordnungen gehören zu den Moduln, die sich selbst konjugiert sind.

Die Definition der *Norm eines Moduls* entnehmen wir einer oben zitierten Brandtschen Arbeit [10]).

Ist ferner $\mathfrak{J} = [\iota_0, \iota_1, \iota_2, \iota_3]$ eine Maximalordnung und $\mathfrak{m}$ irgendein Modul derselben Algebra, mit der Basis $\mu_0, \mu_1, \mu_2, \mu_3$, so werden die μ_i aus den ι_k durch ein eindeutig bestimmtes Gleichungssystem $\mu_i = \sum_{k=0}^{3} m_{ki}\iota_k$ mit rationalen m_{ki} bestimmt. Die absolut genommene Determinante $|m_{ki}| = |\mathfrak{m}|$ heißt dann die *Determinante* von $\mathfrak{m}$. Ihr Wert ist von der Basis von $\mathfrak{m}$ und $\mathfrak{J}$, ja von $\mathfrak{J}$ selbst unabhängig.

Dem Modul $\mathfrak{m} = [\mu_0, \mu_1, \mu_2, \mu_3]$ kann ferner die negativ genommene Determinante $-|s(\mu_i\mu_k)| = D(\mathfrak{m})$ zugeordnet werden, sie heißt die *Diskriminante* von $\mathfrak{m}$. Die Diskriminante eines Moduls ist immer eine Quadratzahl. Enthält $\mathfrak{m}$ nur Zahlen mit negativer Diskriminante (z. B. ein Modul des Hamiltonschen Quaternionensystems), so bezeichnen wir $-|\sqrt{D(\mathfrak{m})}|$, sonst $|\sqrt{D(\mathfrak{m})}|$ als die *Grundzahl* von $\mathfrak{m}$. Sie soll stets $d(\mathfrak{m})$ geschrieben werden.

---

[10]) B. III, S. 14.

Die Grundzahl einer Maximalordnung heißt auch die *Grundzahl der Algebra* schlechthin. Die Vorzeichenfestsetzung geschieht hier auf Vorschlag von Herrn Brandt entgegengesetzt der von ihm zuerst getroffenen Festsetzung [11]).

2. Enthält ein Modul $\mathfrak{m}$ nur ganze Größen, so wird er *ganzzahlig* genannt; $\mathfrak{m}$ heißt *ganz*, wenn $\mathfrak{m} \times \mathfrak{m} < \mathfrak{m}$ gilt. Ein ganzer Modul ist stets auch ganzzahlig, denn er ist in seiner Linksordnung $\mathfrak{m}^0$ und in seiner Rechtsordnung $\mathfrak{m}_0$ enthalten. Ordnungen sind aber immer ganzzahlig.

Sind die Ordnungen eines Moduls $\mathfrak{m}$, $\mathfrak{m}_0$ und $\mathfrak{m}^0$, Maximalordnungen, so heißt $\mathfrak{m}$ *Ideal*. Für Ideale fallen die Begriffe „ganz" und „ganzzahlig" zusammen.

Ist $\mathfrak{m}$ ein ganzer Modul, und gibt es keine ganze rationale Zahl $m > 1$ so, daß $\frac{1}{m}\mathfrak{m}$ ein ganzzahliger Modul ist, so heißt $\mathfrak{m}$ ein *eigentlich primitiver* Modul. Ist $\mathfrak{m}$ ganz, aber nicht eigentlich primitiv, und gibt es keine ganze rationale Zahl $m > 1$ so, daß $\frac{1}{m}\mathfrak{m}$ ganz ist, so heißt $\mathfrak{m}$ *uneigentlich primitiv*. Für Ideale fallen diese beiden Primitivitätsbegriffe wieder zusammen.

3. Von der nun folgenden Tatsache wird stets ausgiebig Gebrauch gemacht:

Satz 1. *Jeder ganzzahlige Modul ist in einer Maximalordnung enthalten* [12]).

Beweis. $\mathfrak{m}$ sei ein ganzzahliger Modul. Dann ist auch $[1, \mathfrak{m}] = \mathfrak{n}$ ganzzahlig. $\mathfrak{n}$ enthält mit einer Zahl ν auch die konjugierte $\bar{\nu} = -\nu + s(\nu)$, deshalb ist $\mathfrak{n} = \bar{\mathfrak{n}}$.

Es sei $\nu_0, \nu_1, \nu_2, \nu_3$ eine Basis von $\mathfrak{n}$. Das Produkt $\mathfrak{n} \times \mathfrak{n} = \mathfrak{n} \times \bar{\mathfrak{n}}$ enthält die Zahlen $\nu_i \bar{\nu}_k$ und ihre Summen. Die $\nu_i \bar{\nu}_k$ sind ganz; weil $\mathfrak{n}$ ganzzahlig ist, sind die Zahlen $n(\nu_i \bar{\nu}_k) = n(\nu_i)\, n(\nu_k)$ und $s(\nu_i \bar{\nu}_k) = n(\nu_i, \nu_k)$ nämlich ganz. Sind die $\nu_i \bar{\nu}_k$ außerdem konkordant, so ist $\mathfrak{n} \times \mathfrak{n}$ ebenfalls ein ganzzahliger Modul.

Die $\nu_i \bar{\nu}_k$ sind in der Tat konkordant. Um dies zu zeigen, werde zur Abkürzung

$$n(\nu_i, \nu_k) = n_{ik} \qquad (i, k = 0, 1, 2, 3)$$

und

$$\vartheta = \nu_{i_4} \bar{\nu}_{i_2} n_{i_1 i_2} - \nu_{i_1} \bar{\nu}_{i_2} n_{i_4 i_3} + \nu_{i_2} \bar{\nu}_{i_2} n_{i_1 i_4} - \nu_{i_1} \bar{\nu}_{i_4} n_{i_2 i_3} + \nu_{i_1} \bar{\nu}_{i_3} n_{i_2 i_4} - \nu_{i_1} \bar{\nu}_{i_2} n_{i_3 i_4}$$

gesetzt. Dann ist

$$(1) \qquad n(\nu_{i_1} \bar{\nu}_{i_2}, \nu_{i_4} \bar{\nu}_{i_3}) = 2 \nu_{i_1} \bar{\nu}_{i_2} \nu_{i_3} \bar{\nu}_{i_4} + \vartheta\,.$$

Der Hauptnenner aller $n(\nu_{i_1} \bar{\nu}_{i_2}, \nu_{i_4} \bar{\nu}_{i_3})$ sei t; ferner seien in (1) die Indizes i_1, i_2, i_3, i_4 so gewählt, daß $n(\nu_{i_1} \bar{\nu}_{i_2}, \nu_{i_4} \bar{\nu}_{i_3})$ einen möglichst großen Nenner t_0 hat. Die $n_{i_j i_k}$ sind ganz und rational, folglich sind $s(\vartheta)$ und $n(\vartheta) t$ auch ganz und rational. Aus (1) erhält man nun durch Normenbildung

$$(2) \quad n(\nu_{i_1} \bar{\nu}_{i_2}, \nu_{i_4} \bar{\nu}_{i_3})^2 = n(\nu_{i_1} \bar{\nu}_{i_2}, \nu_{i_4} \bar{\nu}_{i_3})\, s(\vartheta) - n(\vartheta) + 4\, n(\nu_{i_1})\, n(\nu_{i_2})\, n(\nu_{i_3})\, n(\nu_{i_4})\,.$$

[11]) B. III, S. 9.

[12]) Dieser Satz gilt nicht in allgemeinen hyperkomplexen Systemen, wie folgendes Beispiel lehrt: μ_1, μ_2, μ_3 seien die Wurzeln der Gleichung $x^3 + \frac{1}{2} x^2 + \frac{1}{2} x + 1 = 0$, und ε sei eine den Bedingungen

$$\varepsilon^3 = 1, \qquad \varepsilon^{-1} \mu_i \varepsilon = \mu_{i+1} \qquad (\mu_4 = \mu_1)$$

genügende Größe. Jetzt betrachten wir den Modul

$$\mathfrak{m} = [1, \varepsilon, \varepsilon\mu_1]\,.$$

Die Größen $\varepsilon x_1 + \varepsilon \mu_1 x_2$ genügen den Gleichungen

$$(\varepsilon x_1 + \varepsilon \mu_1 x_2)^3 = n(x_1 + \mu_1 x_2) = x_1^3 + \tfrac{1}{2} x_1^2 x_2 + \tfrac{1}{2} x_1 x_2^2 + x_2^3\,,$$

sie sind für ganze rationale x_1, x_2 also ganz. Folglich enthält $\mathfrak{m}$ nur ganze Größen. $\mathfrak{m}$ ist aber nicht in einer Ordnung enthalten, denn diese müßte auch $\mu_1 = \varepsilon^3 \mu_1$ enthalten, μ_1 ist aber nicht ganz.

Die rechte Seite von (2) ergibt, mit t multipliziert, eine ganze rationale Zahl. Da nun t_0 die kleinste ganze rationale Zahl ist, für welche $t_0\ n(v_{i_1}\overline{v}_{i_2}, v_{i_1}'\overline{v}_{i_2})$ ganz ist, ist t_0^2 ein Teiler von t. Das widerspricht der vorausgesetzten Maximaleigenschaft von t_0, außer in dem Falle $t = t_0 = 1$, d. h. dann, wenn die $v_i\overline{v}_k$ konkordant sind.

$\mathfrak{n} \times \mathfrak{n}$ ist also ganzzahlig. Analog zeigt man dann, daß $(\mathfrak{n} \times \mathfrak{n}) \times (\mathfrak{n} \times \mathfrak{n})$ ganzzahlig ist. So folgt schließlich, daß die Reihe der Moduln $\mathfrak{n}, \mathfrak{n} \times \mathfrak{n}, \mathfrak{n} \times \mathfrak{n} \times \mathfrak{n}, \ldots$, die der Kürze halber auch $\mathfrak{n}, \mathfrak{n}^2, \mathfrak{n}^3, \ldots$ geschrieben werden mögen, unendlich viele ganzzahlige Moduln enthält. Jeder Modul dieser Reihe umfaßt alle vor ihm stehenden; aus dem Grund sind alle diese Moduln ganzzahlig.

Die Diskriminanten dieser Moduln bilden eine absteigende Reihe ganzer rationaler positiver von Null verschiedener Zahlen; daher können es nur endlich viele verschiedene sein. Folglich sind auch nur endlich viele der Moduln $\mathfrak{n}, \mathfrak{n}^2, \ldots$ verschieden. Für ein gewisses n sei $\mathfrak{n}^n = \mathfrak{n}^{n+1}$, dann ist $\mathfrak{n}^n \times \mathfrak{n}^n = \mathfrak{n}^n$; weil $\mathfrak{n}$ die 1 enthält, ist jetzt $\mathfrak{n}^n$ eine Ordnung.

$\mathfrak{n}^n$ ist die kleinste Ordnung, die $\mathfrak{n}$ enthält. Entweder ist $\mathfrak{n}^n$ selber Maximalordnung oder läßt sich zu einer Maximalordnung erweitern. Damit ist der Satz 1 bewiesen.

§ 2. Der reziproke Modul.

1. Das nächste Ziel ist in diesem Paragraphen der Beweis von

Satz 2. $\mathfrak{m}$ *ist dann und nur dann umkehrbar, wenn der reziproke Modul* $\mathfrak{m}^{-1}$ *von* $\mathfrak{m}$ *gleich dem konjugierten Modul ist, dividiert durch die Norm, also wenn*

$$\mathfrak{m}^{-1} = \frac{1}{n(\mathfrak{m})}\,\overline{\mathfrak{m}}\,.$$

Es genügt offenbar, den Satz für ganze Moduln zu beweisen. Ist nämlich $\mathfrak{m}$ ein beliebiger Modul, so gibt es eine ganze rationale Zahl M so, daß $M\mathfrak{m}$ ganz ist; dann ist $(M\mathfrak{m})^{-1} = \frac{1}{M}\,\mathfrak{m}^{-1}$, $\frac{\overline{M\mathfrak{m}}}{n(M\mathfrak{m})} = \frac{1}{M}\frac{\overline{\mathfrak{m}}}{n(\mathfrak{m})}$. Es ist also $\mathfrak{m}^{-1} = \frac{1}{n(\mathfrak{m})}\,\overline{\mathfrak{m}}$ dann und nur dann, wenn $(M\mathfrak{m})^{-1} = \frac{\overline{M\mathfrak{m}}}{n(M\mathfrak{m})}$ ist.

In diesem ganzen Paragraphen bedeutet $\mathfrak{m}$ einen ganzen Modul der Linksordnung $\mathfrak{m}^0 = \mathfrak{o}_1$, der Rechtsordnung $\mathfrak{m}_0 = \mathfrak{o}_2$ und der Norm $n(\mathfrak{m}) = m$. Ist $f((x))$ die Normenform[13]) von $\mathfrak{m}$, so werden die Normen aller Zahlen aus $\mathfrak{m}$ durch $m\,f((x))$ dargestellt. $f((x))$ ist eine Form ohne Koeffiziententeiler und stellt daher Zahlen dar, die zu einer gegebenen Zahl, z. B. m, teilerfremd sind. Entsprechend enthält $\mathfrak{m}$ eine Zahl μ mit $\left(\frac{n(\mu)}{m}, m\right) = 1$. Aus diesem Grunde ist m der g. g. T. der Normen aller Zahlen aus $\mathfrak{m}$. Weil $\mathfrak{m}$ ganz ist, ist $\mathfrak{m} < \mathfrak{m}_0 = \overline{\mathfrak{m}}_0$, also $\overline{\mathfrak{m}} < \mathfrak{m}_0$, $\overline{\mathfrak{m}} \times \mathfrak{m} < \mathfrak{m}$, d. h. $\mathfrak{m}$ enthält mit einer Zahl μ' auch $n(\mu') = \overline{\mu}'\mu'$ und deren g. g. T. m.

Der Beweis des Satzes 2 steht in engstem Zusammenhang mit dem

Satz 3. *Ein ganzer Modul* $\mathfrak{m}$ *ist dann und nur dann umkehrbar, wenn* $\mathfrak{m}$ *mit dem Modul*

$$\mathfrak{m}_1 = \mathfrak{o}_1\,n(\mathfrak{m}) + \mathfrak{o}_1\mu \tag{3}$$

übereinstimmt; dabei möge $\frac{n(\mu)}{n(\mathfrak{m})}$ *zu* $n(\mathfrak{m})$ *teilerfremd sein.*

---

[13]) B. III, S. 13, 14.

2. *Beweise.* Wir beginnen mit der Untersuchung von $\mathfrak{m}_1$.

Es ist $\mathfrak{m}_1 < \mathfrak{m}$ und daher $n(\mathfrak{m}_1)$ durch $n(\mathfrak{m})$ teilbar. Andererseits teilt $n(\mathfrak{m}_1)$ sowohl $n(\mu)$ wie $n(m) = m^2$; wegen $\left(\frac{n(\mu)}{m}, m\right) = 1$ ist der g. g. T. von $n(\mu)$ und m^2 gleich m, mithin ist

$$n(\mathfrak{m}_1) = m\,.$$

Ferner ist (vgl. § 1, **1**, Absatz 4)

$$\mathfrak{m}_1 \times \overline{\mathfrak{m}}_1 \frac{1}{m} = \frac{1}{m}\,\mathfrak{o}_1 \times [m, \mu] \times [\overline{\mu}, m] \times \mathfrak{o}_1 = \mathfrak{o}_1 \times [1, \mu] \times \mathfrak{o}_1;$$

$\mathfrak{m}$ war als ganz vorausgesetzt, daher gilt $\mathfrak{m} < \mathfrak{o}_1$, insbesondere $\mu < \mathfrak{o}_1$ und wegen der letzten Gleichung

$$\mathfrak{m}_1 \times \overline{\mathfrak{m}}_1 \frac{1}{m} = \mathfrak{o}_1\,. \tag{4}$$

Zugleich sieht man, daß $\mathfrak{o}_1$ die Linksordnung von $\mathfrak{m}_1$ ist.

Bezeichnet $\mathfrak{o}_2'$ die Rechtsordnung von $\mathfrak{m}_1$, so gilt auch

$$\frac{1}{m}\,\overline{\mathfrak{m}}_1 \times \mathfrak{m}_1 = \mathfrak{o}_2'\,. \tag{5}$$

Es ist nämlich nach (4) $\mathfrak{m}_1 \times \overline{\mathfrak{m}}_1 \frac{1}{m} \times \mathfrak{m}_1 = \mathfrak{m}_1$, also $\frac{1}{m}\,\overline{\mathfrak{m}}_1 \times \mathfrak{m}_1 < \mathfrak{o}_2'$. Andererseits enthält $\frac{1}{m}\,\overline{\mathfrak{m}}_1 \times \mathfrak{m}_1$ die Zahlen $\frac{m^2}{m} = m$ und $\frac{\overline{\mu}\mu}{m} = \frac{n(\mu)}{m}$ und deren g. g. T., welcher gleich 1 ist, d. h. $\frac{1}{m}\,\overline{\mathfrak{m}}_1 \times \mathfrak{m}_1 > 1$. Multiplikation mit $\mathfrak{o}_2'$ ergibt nun auch $\frac{1}{m}\,\overline{\mathfrak{m}}_1 \times \mathfrak{m}_1 > \mathfrak{o}_2'$.

Aus (4) und (5) folgt die Umkehrbarkeit von $\mathfrak{m}_1$, denn $\mathfrak{m}_1^{-1}$ enthält jetzt $\frac{1}{m}\,\mathfrak{m}_1$, es gilt daher erst recht $\mathfrak{m}_1^{-1} \times \mathfrak{m}_1 = \mathfrak{o}_2'$, $\mathfrak{m}_1 \times \mathfrak{m}_1^{-1} = \mathfrak{o}_1$. Damit ist der erste Teil des Satzes 3 bewiesen.

Der Modul $\frac{1}{m}\,\overline{\mathfrak{m}}_1 \times \mathfrak{m}_1 \times \mathfrak{m}_1^{-1}$ ist einerseits gleich $\mathfrak{m}^{-1}$ wegen (5), andererseits wegen der Umkehrbarkeit von $\mathfrak{m}_1$ gleich $\frac{1}{m}\,\overline{\mathfrak{m}}_1$, für $\mathfrak{m}_1$ gilt also Satz 2 und

$$\mathfrak{m}_1^{-1} = \mathfrak{o}_1 + \frac{\overline{\mu}}{m}\,\mathfrak{o}_1\,. \tag{6}$$

Wegen dieser Bemerkung folgt Satz 2 sofort aus Satz 3.

3. Jetzt kommen wir zur Untersuchung des Moduls

$$\mathfrak{m}_2 = \mathfrak{m}_1^{-1} \times \mathfrak{m}\,. \tag{7}$$

Aus **2** folgt gleich

$$\mathfrak{m} = \mathfrak{m}_1 \times \mathfrak{m}_2\,. \tag{8}$$

Zunächst müssen wir wissen, daß $\mathfrak{m}_2$ ganzzahlig ist. Nach (6) ist

$$\mathfrak{m}_2 = \mathfrak{m} + \frac{\overline{\mu}}{m}\,\mathfrak{m}\,.$$

$\frac{\overline{\mu}}{m}\,\mathfrak{m}$ ist ganzzahlig; $\frac{\overline{\mu}}{m}\,\mathfrak{m}$ besteht nämlich aus allen Zahlen $\frac{\overline{\mu}\mu'}{m}$, wo μ' alle Zahlen aus

$\mathfrak{m}$ durchläuft. Ihre Spuren und Normen sind

$$s\left(\frac{\bar{\mu}\,\mu'}{m}\right) = \frac{n(\mu, \mu')}{m}, \qquad n\left(\frac{\bar{\mu}\,\mu'}{m}\right) = \frac{n(\mu)\, n(\mu')}{m},$$

also ganz, d. h. alle Zahlen aus $\frac{\bar{\mu}}{m}\,\mathfrak{m}$ sind ganz.

$\mathfrak{o}_2$ ist die Rechtsordnung von $\frac{\bar{\mu}}{m}\,\mathfrak{m}$; aus diesem Grunde sind alle Zahlen aus $\mathfrak{o}_2$ mit denen aus $\frac{\bar{\mu}}{m}\,\mathfrak{m}$ konkordant. Weil $\mathfrak{m}$ ein ganzer Modul ist, ist $\mathfrak{m} < \mathfrak{o}_2$, und daher sind erst recht die Zahlen aus $\mathfrak{m}$ mit denen aus $\frac{\bar{\mu}}{m}$ konkordant. Folglich ist $\mathfrak{m} + \frac{\bar{\mu}}{m}\,\mathfrak{m}$ ganzzahlig.

Nach (7) und **2** ist

$$\mathfrak{m}_2 > \mathfrak{m}_1^{-1} \times \mathfrak{m}_1 = \mathfrak{o}_2' > 1,$$

$\mathfrak{m}_2$ enthält die 1. Da nach (7) und (8) $\mathfrak{o}_2$ die Rechtsordnung von $\mathfrak{m}_2$ ist, kann man mit $\mathfrak{o}_2$ multiplizieren, und es folgt sogar

$$\mathfrak{m}_2 > \mathfrak{o}_2 . \tag{9}$$

Weil $\mathfrak{m}_2$ ganzzahlig ist und die 1 enthält, liegt mit einer Zahl α auch die konjugierte $\bar{\alpha} = s(\alpha) - \alpha$ in $\mathfrak{m}_2$. Daher ist $\mathfrak{m}_2 = \bar{\mathfrak{m}}_2$, und folglich ist $\mathfrak{o}_2$ auch die Linksordnung von $\mathfrak{m}_2$.

4. Es werde jetzt $\mathfrak{m}$ als umkehrbar vorausgesetzt. Dann ist auch $\mathfrak{m}_2$ umkehrbar und $\mathfrak{m}_2^{-1} = \mathfrak{m}^{-1} \times \mathfrak{m}_1$,

$$\mathfrak{m}_2^{-1} \times \mathfrak{m}_2 = \mathfrak{m}_2 \times \mathfrak{m}_2^{-1} = \mathfrak{o}_2 . \tag{10}$$

Die Reihe der Moduln $\mathfrak{m}_2, \mathfrak{m}_2 \times \mathfrak{m}_2, \ldots$ enthält nach dem Vorhergehenden und § 1, **3** sicher eine Ordnung $\mathfrak{o} = \mathfrak{m}_2^k$. $\mathfrak{o}$ umfaßt nach (9) die Ordnung $\mathfrak{o}_2$. Andererseits ist nach (10)

$$\mathfrak{m}_2^k \times (\mathfrak{m}_2^{-1})^k = \mathfrak{o}_2 = \mathfrak{o} \times (\mathfrak{m}_2^{-1})^k ,$$

deshalb ist $\mathfrak{o} \times \mathfrak{o}_2 = \mathfrak{o}_2$, also $\mathfrak{o} = \mathfrak{o}_2 = \mathfrak{m}_2^k$. Aus (9) folgt nun $\mathfrak{m}_2 = \mathfrak{o}_2$, d. h. wegen (8) $\mathfrak{m} = \mathfrak{m}_1$, und damit sind die Sätze 2 und 3 bewiesen.

5. Das wichtigste Kriterium für die Umkehrbarkeit eines Moduls enthält der

Satz 4. *$\mathfrak{m}$ ist dann und nur dann umkehrbar, wenn*

$$|\mathfrak{m}| = |\mathfrak{m}_0|\, n(\mathfrak{m})^2 = |\mathfrak{m}^0|\, n(\mathfrak{m})^2$$

ist. In jedem Falle ist

$$t = \frac{|\mathfrak{m}_0|\, n(\mathfrak{m})^2}{|\mathfrak{m}|} = \frac{|\mathfrak{m}^0|\, n(\mathfrak{m})^2}{|\mathfrak{m}|}$$

eine ganze rationale Zahl.

Beweis. Wie oben genügt es, sich beim Beweise auf den Fall zu beschränken, daß $\mathfrak{m}$ ein ganzer Modul ist; denn jeder Modul kann durch Multiplikation mit einer ganzen rationalen Zahl in einen ganzen verwandelt werden; dabei bleibt die Zahl t unverändert. An den bisher gebrauchten Bezeichnungen soll festgehalten werden, insbesondere sei wieder $\mathfrak{m}^0 = \mathfrak{o}_1$, $\mathfrak{m}_0 = \mathfrak{o}_2$.

Die Determinante $|M| = \frac{|\mathfrak{m}|}{|\mathfrak{o}_1|}$ einer Substitution M, die eine Basis von $\mathfrak{o}_1$ in eine von $\mathfrak{m}$ transformiert, teilt die Determinanten aller Substitutionen M', die eine Basis

von $\mathfrak{o}_1$ in eine von $\mathfrak{o}_1\mu'$ transformieren, unter μ' Zahlen aus $\mathfrak{m}$ verstanden. Die Determinanten der M' sind $|M'| = n(\mu')^2$, und deren g. g. T. ist m^2, d. h. $\frac{|\mathfrak{m}|}{|\mathfrak{o}_1|}$ teilt m^2.

Ist $\mathfrak{m}$ umkehrbar, so ist nach Satz 2 und 3

$$\mathfrak{o}_1 m = \mathfrak{m} \times \overline{\mathfrak{m}} = (\mathfrak{m}m + \mathfrak{m}\bar{\mu}) \times \mathfrak{o}_1 > \mathfrak{m}m + \mathfrak{m}\bar{\mu} .$$

Die Determinante $|N| = \frac{|\mathfrak{o}_1 m|}{|\mathfrak{m}|}$ der Substitution N, die eine Basis von $\mathfrak{m}$ in eine von $\mathfrak{o}_1 m$ transformiert, teilt die Determinanten der Substitutionen N_1 bzw. N_2, welche eine Basis von $\mathfrak{m}$ in eine von $\mathfrak{m}m$ bzw. $\mathfrak{m}\bar{\mu}$ transformieren. Diese Determinanten sind $|N_1| = n(m)^2 = m^4$ bzw. $|N_2| = n(\mu)^2$, ihr g. g. T. ist m^2, also $\frac{|\mathfrak{o}_1 m|}{|\mathfrak{m}|}$ teilt m^2. Nun ist aber $\frac{|\mathfrak{o}_1 m|}{|\mathfrak{m}|} = m^4 \frac{|\mathfrak{o}_1|}{|\mathfrak{m}|}$, also $\frac{|\mathfrak{m}|}{|\mathfrak{o}_1|}$ ist durch m^2 teilbar, und nach dem Vorhergehenden $\frac{|\mathfrak{m}|}{|\mathfrak{o}_1|} = m^2$.

Dasselbe gilt, wenn $\mathfrak{o}_1$ durch $\mathfrak{o}_2$ ersetzt wird.

Ist $\mathfrak{m}$ nicht umkehrbar, so gilt jetzt für $\mathfrak{m}_1$

$$|\mathfrak{m}_1| = |\mathfrak{o}_1|\, n(\mathfrak{m}_1)^2 = |\mathfrak{o}_2'|\, n(\mathfrak{m}_1)^2 ,$$

wenn $\mathfrak{o}_2'$, wie in **2**, die Rechtsordnung von $\mathfrak{m}_1$ bezeichnet. Nach (7) ist $\mathfrak{o}_2' \times \mathfrak{m}_2 = \mathfrak{m}_2$, und da $\mathfrak{o}_2$ in **3** als die Linksordnung und Rechtsordnung von $\mathfrak{m}_2$ erkannt wurde, ist $\mathfrak{o}_2' < \mathfrak{o}_2$. Also

$$|\mathfrak{o}_1| = |\mathfrak{o}_2'| \geqq |\mathfrak{o}_2| .$$

Aus Symmetriegründen gilt aber auch $|\mathfrak{o}_2| \geqq |\mathfrak{o}_1|$, also $|\mathfrak{o}_1| = |\mathfrak{o}_2|$ und $\mathfrak{o}_2 = \mathfrak{o}_2'$.

Wenn nun $\mathfrak{m}$ nicht umkehrbar ist, so geht $\mathfrak{m}_1$ aus $\mathfrak{m}$ durch eine ganzzahlige lineare Substitution der Determinante $t > 1$ hervor, und nach dem Vorhergehenden ist

$$t = \frac{|\mathfrak{m}_1|}{|\mathfrak{m}|} = \frac{|\mathfrak{o}_1|\, n(\mathfrak{m}_1)^2}{|\mathfrak{m}|} = \frac{|\mathfrak{o}_2|\, n(\mathfrak{m}_1)^2}{|\mathfrak{m}|} = \frac{|\mathfrak{m}^0|\, n(\mathfrak{m})^2}{|\mathfrak{m}|} = \frac{|\mathfrak{m}_0|\, n(\mathfrak{m})^2}{|\mathfrak{m}|} .$$

Damit ist Satz 4 bewiesen.

6. Zum Schluß dieses Paragraphen sei noch auf zwei Tatsachen hingewiesen, die später benutzt werden sollen.

Erstens. Ist $\mathfrak{m}$ ein ganzer Modul, so ist

$$\frac{1}{n(\mathfrak{m})} \overline{\mathfrak{m}} \times \mathfrak{m} = \overline{\mathfrak{m}}_2 \times \mathfrak{m}_2 = \mathfrak{m}_2 \times \mathfrak{m}_2 .$$

Dies ist nach § 1, **3** ein ganzzahliger Modul, weil $\mathfrak{m}_2$ ganzzahlig ist; wegen (9) enthält er sogar $\mathfrak{o}_2$.

Dies gilt aber auch für einen beliebigen Modul, da ein beliebiger Modul durch Multiplikation mit einer ganzen rationalen Zahl in einen ganzen verwandelt werden kann, wodurch sich $\frac{1}{n(\mathfrak{m})} \overline{\mathfrak{m}} \times \mathfrak{m}$ nicht ändert.

Zweitens. Es werde nach der kleinsten ganzen rationalen (positiven) Zahl m' in $\mathfrak{m}$ gefragt. Ich behaupte, es ist $m' = m$, wenn $\mathfrak{m}$ ein ganzer eigentlich primitiver Modul ist.

Für einen ganzen Modul $\mathfrak{m}$ gilt nämlich, wie in **1** gezeigt wurde, $n(\mathfrak{m}) < \mathfrak{m}$, also ist $m' \leqq m$, und zwar ist m' ein Teiler von m.

Ist $\mathfrak{m}$ ein Ideal, so ist $\mathfrak{m}$ umkehrbar, und nach Satz 3 kann man schreiben $\mathfrak{m} = \mathfrak{o}_1 m + \mathfrak{o}_1 \mu = \mathfrak{o}_1 \times [m, \mu]$, und da m' in $\mathfrak{m}$ liegt und in m aufgeht, ist auch $\mathfrak{m} = \mathfrak{o}_1 \times [m', \mu]$. Der Modul $[m', \mu]$ ist, ebenso wie $\mathfrak{m}$, ganz und eigentlich primitiv;

seine Norm kann nicht kleiner als m sein. Daraus folgt $m' \geqq m$. Die Behauptung $m = m'$ gilt daher für Ideale.

Es sei jetzt $\mathfrak{m}$ ein beliebiger ganzer eigentlich primitiver Modul, dann ist nach dem ersten Teil von **6** $\frac{1}{m}\,\overline{\mathfrak{m}} \times \mathfrak{m}$ ein ganzzahliger Modul, und es gilt $\mathfrak{m} < \mathfrak{o}_2 < \frac{1}{m}\,\overline{\mathfrak{m}} \times \mathfrak{m}$. $\mathfrak{J}$ möge eine $\frac{1}{m}\,\overline{\mathfrak{m}} \times \mathfrak{m}$ enthaltende Maximalordnung sein. Jetzt ist

$$\mathfrak{J} = \mathfrak{J} \times \left(\frac{1}{m}\,\overline{\mathfrak{m}} \times \mathfrak{m}\right) \times \mathfrak{J} = \frac{1}{m}\,(\overline{\mathfrak{m} \times \mathfrak{J}}) \times (\mathfrak{m} \times \mathfrak{J}).$$

Aber auch $\frac{1}{n(m \times \mathfrak{J})}\,(\overline{\mathfrak{m} \times \mathfrak{J}}) \times (\mathfrak{m} \times \mathfrak{J})$ ist ein ganzzahliger $\mathfrak{J}$ umfassender Modul, der wegen der Maximaleigenschaft von $\mathfrak{J}$ mit $\mathfrak{J}$ identisch sein muß. Vergleich mit der letzten Formel lehrt dann $n(\mathfrak{m}) = m = n(\mathfrak{m} \times \mathfrak{J})$.

Nun ist auch $\mathfrak{m} \times \mathfrak{J}$ ganz und primitiv, und daher $n(\mathfrak{m} \times \mathfrak{J})$ die kleinste rationale in $\mathfrak{m} \times \mathfrak{J}$ enthaltene Zahl, sie ist kleiner oder gleich der kleinsten rationalen Zahl m' in $\mathfrak{m}$. Oben war schon $m' \leqq m$ gezeigt, somit folgt nun $m' = m = n(\mathfrak{m})$, w. z. b. w.

II. Abschnitt.
Komplement und Führer von Quaternionenordnungen.
§ 3. Das Komplement einer Ordnung.

1. Es sei $\mathfrak{r} = [\varrho_0, \varrho_1, \varrho_2, \varrho_3]$ ein beliebiger Modul, dann werden durch die linearen Gleichungen

$$\varrho_k = \sum_{i=0}^{3} s(\varrho_i \varrho_k)\,\sigma_i$$

vier linear unabhängige Größen $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ bestimmt. Der Modul $\tilde{\mathfrak{r}} = [\sigma_0, \sigma_1, \sigma_2, \sigma_3]$ heißt das *Komplement* von $\mathfrak{r}$. Das Komplement hat folgende wichtige Grundeigenschaften, die sogar für Moduln beliebiger halbeinfacher Systeme von Herrn Brandt nach dem Vorgange von Dedekind [4]) in einer Vorlesung entwickelt worden sind:

1) $\tilde{\mathfrak{r}}$ ist durch den Modul $\mathfrak{r}$ eindeutig bestimmt.

2) Ist $\mathfrak{r}$ eine Ordnung, so ist $\tilde{\mathfrak{r}}$ der umfassendste Modul, für den $\mathfrak{r} \times \tilde{\mathfrak{r}} < \tilde{\mathfrak{r}}$ bzw. $\tilde{\mathfrak{r}} \times \mathfrak{r} < \tilde{\mathfrak{r}}$ gilt, und dessen Zahlen, mit Zahlen aus $\mathfrak{r}$ multipliziert, ganze Spuren haben. $\mathfrak{r}$ ist die Linksordnung und Rechtsordnung von $\tilde{\mathfrak{r}}$.

3) Die σ_k genügen den Gleichungen

$$s(\varrho_i \sigma_k) = \begin{cases} 0 & \text{für} \quad i \neq k, \\ 1 & \text{für} \quad i = k \end{cases}$$

und sind dadurch eindeutig bestimmt.

4) Für jede Zahl α des Systems gilt

$$\alpha = \sum_{i=0}^{3} s(\alpha \sigma_i)\,\varrho_i.$$

Eine weitere Eigenschaft folgt aus der Definition des Komplements unmittelbar:

5) $$\tilde{\tilde{\mathfrak{r}}} = \tilde{\tilde{\mathfrak{r}}};$$

ist insbesondere $\mathfrak{r}$ eine Ordnung, so ist $\tilde{\tilde{\mathfrak{r}}} = \tilde{\tilde{\mathfrak{r}}} = \tilde{\mathfrak{r}}$.

2. Besonders wichtig und auch leicht zu berechnen ist das Komplement $\tilde{\mathfrak{o}} = [\sigma_0, \sigma_1, \sigma_2, \sigma_3]$ einer Quaternionenordnung $\mathfrak{o}$, wenn man von einer reduzierten Basis $1, \varrho_1, \varrho_2, \varrho_3$ von $\mathfrak{o}$ ausgeht.

Man beachte, daß nach **1**, 2) $\varrho_1\sigma_1$ in $\tilde{\mathfrak{o}}$ liegt. Das bedeutet, es gibt ganze rationale Zahlen a_0, a_1, a_2, a_3 so, daß $\varrho_1\sigma_1 = a_0\sigma_0 + a_1\sigma_1 + a_2\sigma_2 + a_3\sigma_3$ ist. Wegen

$$s(\varrho_1\sigma_1) = s(\sigma_0) = 1,\ s(\sigma_1) = s(\sigma_2) = s(\sigma_3) = 0$$

ist jetzt $a_0 = 1$, und folglich liegt $\sigma_0 = \varrho_1\sigma_1 - a_1\sigma_1 - a_2\sigma_2 - a_3\sigma_3$ in $\mathfrak{o}\sigma_1 + \mathfrak{o}\sigma_2 + \mathfrak{o}\sigma_3$. Somit ist die erste der Formeln

$$\tilde{\mathfrak{o}} = \mathfrak{o}\sigma_1 + \mathfrak{o}\sigma_2 + \mathfrak{o}\sigma_3 = \sigma_1\mathfrak{o} + \sigma_2\mathfrak{o} + \sigma_3\mathfrak{o} \tag{11}$$

bewiesen, die zweite folgt analog.

Zur Vereinfachung der weiteren Rechnungen werde die Verabredung getroffen, daß alle vorkommenden Indizes die Werte 1, 2, 3 durchlaufen sollen und modulo 3 reduziert zu nehmen sind; z. B. soll also $\varrho_4 = \varrho_1$, $\varrho_5 = \varrho_2$ sein. Zweitens sollen $\iota_1, \iota_2, \iota_3$ die Basiseinheiten der Hamiltonschen Quaternionen bedeuten, und es sei

$$\varrho_k = \tfrac{1}{2}\, s(\varrho_k) + \sum_{i=1}^{3} t_{ik}\,\iota_i\,; \tag{12}$$

dabei ist natürlich

$$|t_{ik}| = \pm\tfrac{1}{4}\, d(\mathfrak{o})\,,$$

wo durch eventuelle Vertauschung von ϱ_1 und ϱ_2 erreicht werden kann, daß das positive Vorzeichen steht.

Jetzt wird

$$\tau_k = \frac{\varrho_{k+2}\varrho_{k+1} - \varrho_{k+1}\varrho_{k+2}}{d(\mathfrak{o})} = \frac{1}{d(\mathfrak{o})}\sum_{i=1}^{3}\frac{\partial|t_{rs}|}{\partial t_{ik}}\,2\iota_i; \tag{13}$$

daraus folgt einmal sofort $s(\tau_k) = 0$, zweitens durch Multiplikation von (12) und (13)

$$s(\tau_k\varrho_i) = 4\sum_{l=1}^{3} t_{li}\,\frac{\partial|t_{rs}|}{\partial t_{lk}} = \begin{cases} 0 & \text{für } i \neq k \\ 1 & \text{für } i = k. \end{cases}$$

Nach **1**, 4) ist aus diesem Grunde

$$\sigma_k = \frac{\varrho_{k+2}\varrho_{k+1} - \varrho_{k+1}\varrho_{k+2}}{d(\mathfrak{o})}\ ^{14}) \qquad (k = 1, 2, 3)\,. \tag{14}$$

3. Es soll jetzt das Modulprodukt $\tilde{\mathfrak{o}} \times \tilde{\mathfrak{o}}\, d(\mathfrak{o}) = \hat{\mathfrak{o}} \times \tilde{\mathfrak{o}}\, d(\mathfrak{o})$ berechnet werden.

Nach **1**, 4) haben die σ_k $(k = 1, 2, 3)$ verschwindende Spuren, deshalb sind ihre Quadrate rational, und es gilt

$$d(\mathfrak{o})\,\sigma_k^2 = \tfrac{1}{2}\, s(\sigma_k^2)\, d(\mathfrak{o}) \qquad (k = 1, 2, 3). \tag{15}$$

Die Produkte $\sigma_i\sigma_k$ $(i \neq k)$ ergeben sich folgendermaßen: Wegen $s(\sigma_k) = 0$ ist $\bar{\sigma}_k = -\sigma_k$ und $\overline{\sigma_k\sigma_{k+1}} = \bar{\sigma}_{k+1}\bar{\sigma}_k = \sigma_{k+1}\sigma_k$. Demnach ist

$$\sigma_k\sigma_{k+1} - \sigma_{k+1}\sigma_k = \sigma_k\sigma_{k+1} - \overline{\sigma_k\sigma_{k+1}} = 2\,\sigma_k\sigma_{k+1} - s(\sigma_k\sigma_{k+1})\,.$$

Andererseits ist nach (13)

$$\sigma_k\sigma_{k+1} - \sigma_{k+1}\sigma_k = \frac{2}{d(\mathfrak{o})}\sum_{i=1}^{3} t_{i,k+2}\,\iota_i = \frac{2}{d(\mathfrak{o})}\left(\varrho_{k+2} - \frac{s(\varrho_{k+2})}{2}\right),$$

woraus sich jetzt

$$d(\mathfrak{o})\,\sigma_k\sigma_{k+1} = \varrho_{k+2} + \tfrac{1}{2}\,(s(\sigma_k\sigma_{k+1})\,d(\mathfrak{o}) - s(\varrho_{k+2})) \tag{16}$$

---

[14]) In allgemeinen normalen einfachen Systemen gilt die folgende Verallgemeinerung dieser Tatsache: $\mathfrak{o} = [\ldots, \varrho_i, \ldots, \varrho_k, \ldots]$ sei eine Maximalordnung eines normalen einfachen hyperkomplexen Systems über einem Zahlkörper, $d(\mathfrak{o})$ sei das Produkt der Zentrumsprimideale, welche die Diskriminante von $\mathfrak{o}$ teilen. Dann ist das Komplement von $\mathfrak{o}$ gleich dem Modul $d(\mathfrak{o})^{-1}[\ldots, \varrho_i\varrho_k - \varrho_k\varrho_i, \ldots]$.

ergibt. Analog erhält man

$$(16') \qquad d(\mathfrak{o})\,\sigma_{k+1}\sigma_k = -\varrho_{k+2} + \tfrac{1}{2}\,(s(\sigma_k\sigma_{k+1})\,d(\mathfrak{o}) + s(\varrho_{k+2}))\,.$$

Aus (15), (16), (16′) ließe sich $\tilde{\mathfrak{o}} \times \tilde{\mathfrak{o}}\,d(\mathfrak{o})$ wegen (11) schon berechnen, wenn man wüßte, daß die in diesen Gleichungen auftretenden Koeffizienten ganz sind; das wird jedoch erst in der nächsten Nummer gezeigt werden.

Zunächst soll noch das Verhalten von σ_0 in dem Modulprodukt $\tilde{\mathfrak{o}} \times \tilde{\mathfrak{o}}\,d(\mathfrak{o})$ beschrieben werden.

Die Zahl $\sigma_0' = \frac{1}{2}\,(1 - s(\varrho_1)\,\sigma_1 - s(\varrho_2)\,\sigma_2 - s(\varrho_3)\,\sigma_3)$ genügt wegen **1**, 3) den Gleichungen $s(\sigma_0') = 1$, $s(\sigma_0'\varrho_1) = 0$, $s(\sigma_0'\varrho_2) = 0$, $s(\sigma_0'\varrho_3) = 0$, es ist daher nach **1**, 4) $\sigma_0' = \sigma_0$:

$$\sigma_0 = \tfrac{1}{2}\,(1 - s(\varrho_1)\,\sigma_1 - s(\varrho_2)\,\sigma_2 - s(\varrho_3)\,\sigma_3)\,.$$

Beachtet man $s(\sigma_0) = 1$, so wird $n(\sigma_0) = \frac{1}{2}\,(1 - s(\sigma_0^2))$, und mit zweimaliger Benutzung von **1**, 4) erhält man

$$(17) \quad d(\mathfrak{o})\,\sigma_0^2 = \tfrac{1}{2}\,d(\mathfrak{o})\,(-1 + 3s(\sigma_0^2)) + d(\mathfrak{o})\,s(\sigma_0\sigma_1)\,\varrho_1 + d(\mathfrak{o})\,s(\sigma_0\sigma_2)\,\varrho_2 + d(\mathfrak{o})\,s(\sigma_0\sigma_3)\,\varrho_3\,.$$

Ferner erhält man nach kurzer Rechnung auf Grund von **1**, 4), (15), (16), (16′), wenn man zur Abkürzung

$$\mathfrak{h}_{0k} = d(\mathfrak{o})\,s(\sigma_0\sigma_k)\,, \qquad (k = 1, 2, 3)$$

$$\begin{Vmatrix} \mathfrak{h}_{11}^* & \mathfrak{h}_{12}^* & \mathfrak{h}_{13}^* \\ \mathfrak{h}_{21}^* & \mathfrak{h}_{22}^* & \mathfrak{h}_{23}^* \\ \mathfrak{h}_{31}^* & \mathfrak{h}_{32}^* & \mathfrak{h}_{33}^* \end{Vmatrix} = \frac{1}{2} \begin{Vmatrix} s(\sigma_1^2)\,d(\mathfrak{o}) & s(\sigma_2\sigma_2)\,d(\mathfrak{o}) + s(\varrho_3) & s(\sigma_3\sigma_1)\,d(\mathfrak{o}) - s(\varrho_2) \\ s(\sigma_1\sigma_2)\,d(\mathfrak{o}) - s(\varrho_3) & s(\sigma_2^2)\,d(\mathfrak{o}) & s(\sigma_3\sigma_2)\,d(\mathfrak{o}) + s(\varrho_1) \\ s(\sigma_1\sigma_3)\,d(\mathfrak{o}) + s(\varrho_2) & s(\sigma_2\sigma_3)\,d(\mathfrak{o}) - s(\varrho_1) & s(\sigma_3^2)\,d(\mathfrak{o}) \end{Vmatrix}$$

setzt, die Formeln

$$(18) \qquad d(\mathfrak{o})\,\sigma_0\sigma_k = \mathfrak{h}_{0k} + \sum_{i=1}^{3} \mathfrak{h}_{ik}^*\,\varrho_i\,,$$

$$(18') \qquad d(\mathfrak{o})\,\sigma_k\sigma_0 = \mathfrak{h}_{0k} + \sum_{i=1}^{3} \mathfrak{h}_{ki}^*\,\varrho_i\,.$$

Bezeichnet $H((x))$ die Normenform von $\mathfrak{o}$ und $\tilde{H}((x))$ die von $\tilde{\mathfrak{o}}$, so liefern die Formeln (15) bis (18′) eine bilineare Substitution $\mathfrak{P}$ von positiver Signatur und Art, welche die Identität

$$H((z)) = (n(\tilde{\mathfrak{o}})\,d(\mathfrak{o}))^2\,\tilde{H}((x))\,\tilde{H}((y))$$

vermittelt [15]).

In der nächsten Nummer wird gezeigt werden, daß $n(\tilde{\mathfrak{o}})\,d(\mathfrak{o})\,\tilde{H}((x))$ der reziproken Form von $H((x))$ äquivalent ist. Folglich wird eine zu $\mathfrak{P}$ *koordinierte* Substitution $\mathfrak{Q}$ die Identität $H((z)) = H((x))\,H((y))$ vermitteln [16]).

$\mathfrak{Q}$ ist das System der Multiplikationszahlen von $\mathfrak{o}$. Wenn sich der hier angegebene Weg zu ihrer Berechnung in der Praxis auch nicht empfiehlt, so trägt er doch manches zum Verständnis des oben zitierten Satzes bei, daß sich die Multiplikationszahlen einer Ordnung aus den Koeffizienten ihrer Normenform berechnen lassen.

4. Wieder sei $\varrho_0, \varrho_1, \varrho_2, \varrho_3$ eine reduzierte Basis von $\mathfrak{o}$, d. h. $\varrho_0 = 1$, und

$$H((x)) = \tfrac{1}{2} \sum_{i,k=0}^{3} g_{ik}\,x_i\,x_k = n(x_0\varrho_0 + x_1\varrho_1 + x_2\varrho_2 + x_3\varrho_3)$$

---

[15]) H. Brandt, Der Kompositionsbegriff bei den quaternären quadratischen Formen, Math. Annalen **91** (1924), S. 300, § 2.

[16]) H. Brandt, Bilineare Transformationen quadratischer Formen, Math. Zeitschr. **17** (1923), S. 151.

die Normenform von $\mathfrak{o}$. Wegen der Identität $n(\varrho_i, \varrho_k) = -s(\varrho_i\varrho_k) + s(\varrho_i)s(\varrho_k)$ gilt

$$(19) \qquad \|s(\varrho_i\varrho_k)\| = \|g_{ik}\| \begin{Vmatrix} 1 & 0 & 0 & 0 \\ s(\varrho_1) & -1 & 0 & 0 \\ s(\varrho_2) & 0 & -1 & 0 \\ s(\varrho_3) & 0 & 0 & -1 \end{Vmatrix}.$$

Zufolge der Definitionsgleichung des Komplements geht $H((x))$ durch $x_k = \sum_{i=0}^{3} s(\varrho_k\varrho_i)\, y_i$ in das $n(\tilde{\mathfrak{o}})$-fache der Normenform $\widetilde{H}((y))$ von $\tilde{\mathfrak{o}}$ über. Eine zu $n(\tilde{\mathfrak{o}})\,\widetilde{H}((y))$ äquivalente Form erhält man nach (19) durch die Substitution $y_k = \sum_{i=1}^{3} g_{ki}\, x_i$. Durch diese Substitution geht aber bekanntlich $H((x))$ in das $D(\mathfrak{o})^{-1}$-fache der Adjungierten von $H((x))$, d. h. in das $d(\mathfrak{o})^{-1}$-fache der Reziproken $\mathfrak{H}((y))$ von $H((x))$ über, d. h. die Formen $n(\tilde{\mathfrak{o}})\,\widetilde{H}((y))$ und $d(\mathfrak{o})^{-1}\,\mathfrak{H}((y))$ sind äquivalent.

Aus dem Grunde ist $t = d(\mathfrak{o})\,n(\tilde{\mathfrak{o}})$ eine ganze rationale Zahl und zwar der Koeffiziententeiler von $\mathfrak{H}((y))$.

Einmal ergibt sich hieraus, weil nach § 2, 6 $\tilde{\mathfrak{o}} \times \bar{\tilde{\mathfrak{o}}}\,\dfrac{1}{n(\tilde{\mathfrak{o}})} = \tilde{\mathfrak{o}} \times \bar{\tilde{\mathfrak{o}}}\,\dfrac{d(\mathfrak{o})}{t}$ ganzzahlig ist, daß alle Zahlen $\sigma_i\sigma_k\, d(\mathfrak{o})$ $(i, k = 0, 1, 2, 3)$ ganz sind. Die Koeffizienten

$$\tfrac{1}{2}\, d(\mathfrak{o})(-1 + 3s(\sigma_0^2)),\ \mathfrak{h}_{0k},\ \mathfrak{h}_{ik}^*$$

der Gleichungen (15) bis (18′) müssen daher auch ganz sein.

Zweitens ergibt sich die Zahl t nach der Definitionsgleichung des Komplements zu

$$t = d(\mathfrak{o})\,n(\tilde{\mathfrak{o}}) = \sqrt{\frac{|\mathfrak{o}|\, n(\tilde{\mathfrak{o}})^2}{|\tilde{\mathfrak{o}}|}};$$

nach Satz 4 gilt also

Satz 5. *$\mathfrak{o}$ ist dann und nur dann umkehrbar, wenn die reziproke Form der Normenform von $\mathfrak{o}$ eine primitive Form ist.*

Ist $\tilde{\mathfrak{o}}$ umkehrbar, so ist $\tilde{\mathfrak{o}} \times \tilde{\mathfrak{o}}\, d(\mathfrak{o}) = \tilde{\mathfrak{o}} \times \bar{\tilde{\mathfrak{o}}}\,\dfrac{1}{n(\tilde{\mathfrak{o}})} = \mathfrak{o}$. Im anderen Falle gibt es ganze rationale Zahlen x_1, x_2, x_3 so, daß

$$\mathfrak{o} \times \mathfrak{o}\,\frac{d(\mathfrak{o})}{t} = \tilde{\mathfrak{o}} \times \bar{\tilde{\mathfrak{o}}}\,\frac{1}{n(\tilde{\mathfrak{o}})} = \left[1, \frac{\varrho_1 + x_1}{t}, \frac{\varrho_2 + x_2}{t}, \frac{\varrho_3 + x_3}{t}\right]$$

ist. Da nämlich $\tilde{\mathfrak{o}} \times \bar{\tilde{\mathfrak{o}}}\,\dfrac{1}{n(\mathfrak{o})}$ ganzzahlig ist, folgt die Behauptung sofort aus (11), (15), (16), (16′).

5. Auch der folgende Satz ist ein brauchbares Kriterium für die Umkehrbarkeit des Komplements einer Ordnung; er wird später angewendet werden.

Satz 6. *$\tilde{\mathfrak{o}}$ ist dann und nur dann umkehrbar, wenn es nicht eine Ordnung $\mathfrak{o}'$ und dazu eine ganze rationale Zahl $t > 1$ gibt derart, daß $\mathfrak{o} = [1, t\mathfrak{o}']$ ist.*

Beweis. Es sei zunächst $\mathfrak{o}$ irgendein ganzzahliger Modul mit der Normenform $H((x)) = \frac{1}{2}\sum_{i=0}^{3} g_{ik}\, x_i\, x_k$. $\mathfrak{H}((y))$ sei die reziproke Form von $H((x))$. t sei eine rationale Zahl derart, daß $\dfrac{1}{t}\,\mathfrak{H}((y))$ eine ganzzahlige Form ohne Koeffiziententeiler ist. $d^2 = |g_{ik}|$ sei die Diskriminante von $\mathfrak{o}$. Schließlich seien t_1, t_2, t_3, t_4 die Elementarteiler der Matrix $\|g_{ik}\|$; t_1 ist die Art der Form $H((x))$ und gleich 1 oder gleich 2 [17]).

[17]) Vgl. hierzu und zu dem Folgenden a. a. O. [15]), § 1, Nr. 2.

p sei eine beliebige Primzahl und p^{n_1}, $p^{n_1+n_2}$, $p^{n_1+n_2+n_3}$, $p^{n_1+n_2+n_3+n_4}$, p^{2N}, p^n die Potenzen von p, welche $t_1, t_2, t_3, t_4, d^2, t$ teilen; n darf dabei auch negativ sein.

Für jedes p ist jetzt

$$4n_1 + 3n_2 + 2n_3 + n_4 = 2N, \tag{20}$$

$$3n_1 + 2n_2 + n_3 \qquad = N + n. \tag{21}$$

Darauf möge $\mathfrak{o}'$ ein ganzzahliger Modul sein, $t^* > 1$ eine ganze rationale Zahl und $\mathfrak{o} = [1, t^*\mathfrak{o}']$. Den Zahlen $n_1, n_2, \ldots, n$ für p und $\mathfrak{o}$ entsprechend seien nun für p und $\mathfrak{o}'$ die Zahlen $n_1', n_2', \ldots, n'$ gebildet. p^{n^*} sei die Potenz von p, die t^* teilt.

Falls p ungerade ist oder $p = 2, t' = t = 2$, hat man

$$n_1 = n_1',\ n_2 \geqq n_2' + 2n^*,\ n_3 \geqq n_3',\ n_4 \geqq n_4';\ N = N' + 3n^*;$$

nach (20) gelten hier überall die Gleichheitszeichen und nach (21) ist

$$n = n' + n^*. \tag{22}$$

Ist aber $p = 2, t' = 1$, so ist $t = 2$ und

$$n_1 = n_1' + 1,\ n_2 \geqq n_2' + 2n^* - 2,\ n_3 \geqq n_3' + 1,\ n_4 \geqq n_4';\ N = N' + 3n;$$

nach (20) gelten wieder überall die Gleichheitszeichen und nach (21) ist auch hier

$$n = n' + n^*. \tag{22'}$$

Aus (22) und (22′) ergibt sich jetzt

$$t = t' t^*. \tag{23}$$

Ist insbesondere $\mathfrak{o}'$ eine Ordnung, so ist die reziproke Form der Normenform von $\mathfrak{o}'$ ganzzahlig. Also ist t' ganz, $\mathfrak{o}$ ist wieder eine Ordnung, und wegen (23) hat die reziproke Form der Normenform von $\mathfrak{o}$ den Koeffiziententeiler $t' t^* > 1$. Nach Satz 5 kann also jetzt $\tilde{\mathfrak{o}}$ nicht umkehrbar sein.

Ist umgekehrt $\tilde{\mathfrak{o}}$ nicht umkehrbar und t^* der Koeffiziententeiler der reziproken Form der Normenform von $\mathfrak{o}$, so ist nach **4**

$$\mathfrak{o} = \left[1, t^*\,\tilde{\mathfrak{o}} \times \tilde{\mathfrak{o}}\,\frac{1}{n(\tilde{\mathfrak{o}})}\right],$$

und $\mathfrak{o}' = \tilde{\mathfrak{o}} \times \tilde{\mathfrak{o}}\,\dfrac{1}{n(\tilde{\mathfrak{o}})}$ ist ein ganzzahliger, die 1 enthaltender Modul. Nach (23) ergibt sich aber, daß die reziproke Form der Normenform von $\mathfrak{o}'$ ganzzahlig ist. Nun läßt die Normenform von $\mathfrak{o}'$ eine Komposition mit sich selber zu [15]); dadurch erweist sich $\mathfrak{o}$ als Ordnung. Damit ist Satz 6 bewiesen.

§ 4. Der Führer von Ordnungen.

1. Es seien $\mathfrak{o}$ und $\mathfrak{o}_1$ zwei beliebige Ordnungen. Dann nennen wir die Modulquotienten (vgl. B. II) $\mathfrak{o}_1\backslash\mathfrak{o}$ und $\mathfrak{o}/\mathfrak{o}_1$ den *Linksführer von* $\mathfrak{o}_1$ *nach* $\mathfrak{o}$ und den *Rechtsführer von* $\mathfrak{o}_1$ *nach* $\mathfrak{o}$. Unmittelbar aus der Definition ergibt sich

$$\mathfrak{o}_1\backslash\mathfrak{o} = \overline{\mathfrak{o}/\mathfrak{o}_1}. \tag{24}$$

Ferner folgt ebenfalls unmittelbar aus der Definition $(\mathfrak{o}_1\backslash\mathfrak{o}) \times \mathfrak{o} = \mathfrak{o}_1\backslash\mathfrak{o}$. Deshalb ist $(\mathfrak{o}_1\backslash\mathfrak{o}) \times (\mathfrak{o}_1\backslash\mathfrak{o}) < \mathfrak{o}_1\backslash\mathfrak{o}$, die Führer sind also ganze Moduln. Ist $\mathfrak{o}_1$ die Linksordnung von $\mathfrak{o}_1\backslash\mathfrak{o}$, so ergibt sich hieraus insbesondere $\mathfrak{o}_1\backslash\mathfrak{o} = \mathfrak{o}_1\backslash(\mathfrak{o}_1 \frown \mathfrak{o})$. Es ist jedoch nicht immer $\mathfrak{o}_1$ die Linksordnung von $\mathfrak{o}_1\backslash\mathfrak{o}$, z. B. dann nicht, wenn $\mathfrak{o} > \mathfrak{o}_1$ gilt; und es ist auch nicht immer $\mathfrak{o}_1\backslash\mathfrak{o} = \mathfrak{o}_1\backslash(\mathfrak{o}_1 \frown \mathfrak{o})$.

Im folgenden wollen wir uns ausschließlich auf den Fall beschränken, daß $\mathfrak{o}$ in $\mathfrak{o}_1$ enthalten ist. Hat überdies $\mathfrak{o}$ umkehrbares Komplement, so ist

$$\mathfrak{o}_1\backslash\mathfrak{o} = d(\mathfrak{o})\tilde{\mathfrak{o}}_1 \times \tilde{\mathfrak{o}}, \qquad \mathfrak{o}/\mathfrak{o}_1 = d(\mathfrak{o})\tilde{\mathfrak{o}} \times \tilde{\mathfrak{o}}_1. \tag{25}$$

Den Beweis stützt man am bequemsten auf die für je zwei Moduln $\mathfrak{m}$, $\mathfrak{n}$ gültige einfache Formel

$$\mathfrak{m}\backslash\mathfrak{n} = \tilde{\mathfrak{m}}/\tilde{\mathfrak{n}},$$

deren Beweis von Dedekind [18]) für Zahlkörper geführt wurde und ohne weiteres auf nichtkommutative Systeme übertragen werden kann. Diese Formel ergibt wegen $\mathfrak{o}_1 > \mathfrak{o}$

$$\mathfrak{o}_1\backslash\mathfrak{o} = \tilde{\mathfrak{o}}_1/\tilde{\mathfrak{o}} = \tilde{\mathfrak{o}}_1 \times \tilde{\mathfrak{o}}^{-1}.$$

Aus § 3, **4** entnimmt man aber $\tilde{\mathfrak{o}}^{-1} = \tilde{\mathfrak{o}}\, d(\mathfrak{o})$, woraus die erste der Gleichungen (25) folgt; die zweite ergibt sich aus dieser und (24).

2. Nun soll auch noch $\mathfrak{o}_1$ umkehrbares Komplement besitzen. Dann ist nach (25)

$$(\mathfrak{o}_1\backslash\mathfrak{o}) \times (\overline{\mathfrak{o}_1\backslash\mathfrak{o}}) \cdot \frac{d(\mathfrak{o}_1)}{d(\mathfrak{o})} = d(\mathfrak{o}_1)d(\mathfrak{o})\tilde{\mathfrak{o}}_1 \times \tilde{\mathfrak{o}} \times \tilde{\mathfrak{o}} \times \tilde{\mathfrak{o}}_1;$$

dies Produkt ist nach § 3 gleich $\mathfrak{o}_1$. $\mathfrak{o}_1$ ist daher die Linksordnung von $\mathfrak{o}_1\backslash\mathfrak{o}$; ferner ist $\mathfrak{o}_1\backslash\mathfrak{o}$ umkehrbar und $(\mathfrak{o}_1\backslash\mathfrak{o})^{-1} = (\overline{\mathfrak{o}_1\backslash\mathfrak{o}})\,\frac{d(\mathfrak{o}_1)}{d(\mathfrak{o})}$. Aus Satz 2 folgt nun deswegen $n(\mathfrak{o}_1\backslash\mathfrak{o}) = \frac{d(\mathfrak{o}_1)}{d(\mathfrak{o})}$; dieser Quotient ist aber auch gleich $n(\mathfrak{o}_1\backslash\mathfrak{o}) = \frac{|\mathfrak{o}|}{|\mathfrak{o}_1|}$.

3. Besonders wichtig für später ist der einfache

Satz 7. *$\mathfrak{o}$, $\mathfrak{o}_1$ seien beliebige Ordnungen und $\mathfrak{o}_1 > \mathfrak{o}$. Ist $\mathfrak{o}_1\backslash\mathfrak{o}$ eigentlich primitiv, so ist $\mathfrak{o}_1$ die Linksordnung von $\mathfrak{o}_1\backslash\mathfrak{o}$, $\mathfrak{o}_1\backslash\mathfrak{o}$ ist ein umkehrbarer Modul der Norm $n(\mathfrak{o}_1\backslash\mathfrak{o}) = \frac{|\mathfrak{o}|}{|\mathfrak{o}_1|}$, und es gilt $\mathfrak{o} = [1, \mathfrak{o}_1\backslash\mathfrak{o}]$.*

Beweis. $\mathfrak{o}_1'$ sei die Linksordnung von $\mathfrak{o}_1\backslash\mathfrak{o}$, sie enthält gewiß $\mathfrak{o}_1$; $\mathfrak{o}'$ bezeichne den Modul $[1, \mathfrak{o}_1\backslash\mathfrak{o}]$.

Nach § 2, **6** ist $n(\mathfrak{o}_1\backslash\mathfrak{o})$ die kleinste rationale (ganze) Zahl in $\mathfrak{o}_1\backslash\mathfrak{o}$. Daher ist

$$|\mathfrak{o}| \leqq |\mathfrak{o}'| = |\mathfrak{o}_1\backslash\mathfrak{o}|\, n(\mathfrak{o}_1\backslash\mathfrak{o})^{-1}, \tag{26}$$

und nach Satz 4 gilt

$$|\mathfrak{o}_1\backslash\mathfrak{o}| \leqq |\mathfrak{o}_1'|\, n(\mathfrak{o}_1\backslash\mathfrak{o})^2 \leqq |\mathfrak{o}_1|\, n(\mathfrak{o}_1\backslash\mathfrak{o})^2. \tag{27}$$

Aus (26) und (27) folgt

$$n(\mathfrak{o}_1\backslash\mathfrak{o}) \geqq \frac{|\mathfrak{o}|}{|\mathfrak{o}_1|}.$$

Da andererseits die Determinante der ganzzahligen linearen Substitution, die eine Basis von $\mathfrak{o}_1$ in eine von $\mathfrak{o}$ transformiert, gleich $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|}$ ist, ist nach Definition des Führers $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|}$ in $\mathfrak{o}_1\backslash\mathfrak{o}$ enthalten, also $n(\mathfrak{o}_1\backslash\mathfrak{o}) \leqq \frac{|\mathfrak{o}|}{|\mathfrak{o}_1|}$. Das ergibt $n(\mathfrak{o}_1\backslash\mathfrak{o}) = \frac{|\mathfrak{o}|}{|\mathfrak{o}_1|}$, und in (26) und (27) stehen nur Gleichheitszeichen. Letzteres bedeutet: $\mathfrak{o}' = \mathfrak{o}$, $\mathfrak{o}_1' = \mathfrak{o}_1$, und $\mathfrak{o}_1\backslash\mathfrak{o}$ ist nach Satz 4 umkehrbar.

III. Abschnitt.
Struktur der Quaternionenordnungen.
§ 5. Primitive Ordnungen.

1. Die Wichtigkeit der Unterscheidung zwischen primitiven und imprimitiven Ordnungen wurde schon in der Einleitung erwähnt. Ein für Theorie und praktische

[18]) D. II, § 9, Nr. 6.

Rechnung wichtiges Kriterium für die primitiven Ordnungen ist in folgendem Satz enthalten:

Satz 8. *Ein ganzzahliger die* 1 *enthaltender Modul* $\mathfrak{m}$ (*also insbesondere eine Ordnung*) *enthält dann und nur dann die Maximalordnung eines quadratischen Körpers, wenn es nicht einen ganzzahligen Modul* $\mathfrak{n}$ *und dazu eine ganze rationale Zahl* $f > 1$ *so gibt, daß* $\mathfrak{m} = [1, f\mathfrak{n}]$ *ist.*

Beweis. Läßt sich $\mathfrak{m}$ in der erwähnten Form schreiben, so kann ersichtlich nicht $\mathfrak{m}$ die Maximalordnung eines quadratischen Zahlkörpers enthalten.

Schwierig ist nur der Beweis der Umkehrung dieser Aussage. Dazu sei $1, \mu_1, \mu_2, \mu_3$ eine Basis von $\mathfrak{m}$. Die Diskriminanten aller Zahlen μ aus $\mathfrak{m}$ bzw. aller Ringe $[1, \mu]$ werden durch die Form

$$(28) \quad s(\mu_1 x_1 + \mu_2 x_2 + \mu_3 x_3)^2 - 4n(\mu_1 x_1 + \mu_2 x_2 + \mu_3 x_3) = t^2 s\ F(x_1, x_2, x_3)$$

dargestellt, wobei $F((x))$ eine ganzzahlige Form ohne Koeffiziententeiler ist, t und s ganze rationale Zahlen sind und s quadratfrei ist.

Die Determinante von $F((x))$ ergibt sich nach kurzer Rechnung zu $D(\mathfrak{m}) \cdot 2^5 t^{-6} s^{-3}$, ist also $\neq 0$. $\mathfrak{m}$ enthält dann und nur dann die Maximalordnung eines quadratischen Zahlkörpers, wenn $t^2 s\, F((x))$ die Diskriminante eines solchen darstellt. Der Beweis des Satzes 8 zerfällt nun in zwei Teile. Erstens: $t^2 s F((x))$ stellt die Diskriminante eines quadratischen Zahlkörpers dar, wenn $t = 1$, oder wenn $t = 2$ und eine der Kongruenzen

$$(29) \qquad \begin{aligned} s F(x_1, x_2, x_3) &\equiv 2 (\mathrm{mod}\ 4)\ , \\ s F(x_1, x_2, x_3) &\equiv 3 (\mathrm{mod}\ 4) \end{aligned}$$

lösbar ist.

Zweitens: ist $t > 2$ oder $t = 2$, aber keine der Kongruenzen (29) lösbar, so gibt es eine ganze rationale Zahl $f > 1$ und einen ganzzahligen Modul $\mathfrak{n}$ derart, daß

$$\mathfrak{m} = [1, f\mathfrak{n}]$$

ist.

2. Wir beginnen mit dem Beweis der zweiten Behauptung.

Es sei zuerst $t > 2$ und p eine ungerade in t aufgehende Primzahl. z sei ganz und rational und genüge der Kongruenz $2z \equiv 1 \pmod{p}$. Nun sind die Spuren aller Zahlen

$$\xi = \frac{\mu_1 - z s(\mu_1)}{p} x_1 + \frac{\mu_2 - z s(\mu_2)}{p} x_2 + \frac{\mu_3 - z s(\mu_3)}{p} x_3\ ,$$

wo x_1, x_2, x_3 ganz und rational sind, ganz; und wegen

$$p^2(s(\xi)^2 - 4n(\xi)) = t^2 s F(x_1, x_2, x_3) \equiv 0 \pmod{p}$$

sind auch deren Normen ganz. Dann ist

$$\mathfrak{n} = \left[1, \frac{\mu_2 - z s(\mu_1)}{p}, \frac{\mu_2 - z s(\mu_2)}{p}, \frac{\mu_3 - z s(\mu_3)}{p}\right]$$

ein ganzzahliger Modul und $\mathfrak{m} = [1, p\mathfrak{n}]$.

Ist t gerade, so sind nach (28) $s(\mu_1), s(\mu_2), s(\mu_3)$ gerade; in diesem Falle kann man sich die Basis von $\mathfrak{m}$ durch die folgende

$$1, \mu_1 - \tfrac{1}{2} s(\mu_1),\ \ \mu_2 - \tfrac{1}{2} s(\mu_2),\ \ \mu_3 - \tfrac{1}{2} s(\mu_3)$$

ersetzt denken, kann also ohne Beschränkung der Allgemeingültigkeit $s(\mu_1), s(\mu_2), s(\mu_3) = 0$ annehmen.

Ist t durch 4 teilbar, so ist jetzt $\mathfrak{n} = [1, \tfrac{1}{2}\mu_1, \tfrac{1}{2}\mu_2, \tfrac{1}{2}\mu_3]$ ganzzahlig und $\mathfrak{m} = [1, 2\mathfrak{n}]$.

Schließlich sei $t = 2$, aber keine der Kongruenzen (29) lösbar. Dann lehrt eine elementare Diskussion, daß $sF((x))$ durch eine ganzzahlige Substitution in eine Form $\sum_{i,k=1}^{3} a_{ik} x_i x_k$ transformiert werden kann, für welche

$$a_{ik} \equiv \begin{cases} 1 \pmod 4 & \text{für } i = k = 1, \\ 0 \pmod 4 & \text{für } i = k \neq 1, \\ 0 \pmod 2 & \text{für } i \neq k \end{cases}$$

gilt. Diese Substitution entspricht dem Übergang zu einer neuen Basis: $\mathfrak{m} = [1, \mu_1', \mu_2', \mu_3']$. Für diese muß dann aber $\mathfrak{n} = [1, \frac{1}{2}(1 + \mu_1'), \frac{1}{2}\mu_2', \frac{1}{2}\mu_3']$ ganzzahlig sein und $\mathfrak{m} = [1, 2\mathfrak{n}]$.

3. Es sei jetzt $t = 1$ oder $t = 2$ und eine der Kongruenzen (29) lösbar. Im zweiten Falle darf ohne Beschränkung der Allgemeinheit angenommen werden, daß eine der Kongruenzen (29) durch $x_1 = 1$, $x_2 = 0$, $x_3 = 0$ gelöst wird.

Jetzt ist

$$f(x_1, x_2, x_3) = \begin{cases} F(x_1, x_2, x_3) & \text{für } t = 1, \\ F(x_1, 4x_2, 4x_3) & \text{für } t = 2,\ F(1, 0, 0) \not\equiv 0 \pmod 2, \\ \frac{1}{2}F(x_1, 4x_2, 4x_3) & \text{für } t = 2,\ F(1, 0, 0) \equiv 0 \pmod 2 \end{cases}$$

eine ganzzahlige quadratische Form ohne Koeffiziententeiler.

Ich behaupte, $f((x))$ stellt unendlich viele Primzahlen dar. Für den Augenblick sei die Behauptung als wahr angenommen. Dann erteile man den x_1, x_2, x_3 solche Werte, daß $f((x))$ eine zu $2s$ teilerfremde Primzahl ist. Jetzt wird $sF(x_1, x_2, x_3)$ bzw. $sF(x_1, 4x_2, 4x_3)$ eine quadratfreie Zahl sein, welche für $t = 2$ noch kongruent 2 oder 3 mod 4 ist. Dann ist wirklich $t^2 sF(x_1, x_2, x_3)$ bzw. $t^2 sF(x_1, 4x_2, 4x_3)$ die Diskriminante eines quadratischen Zahlkörpers.

Es bleibt nun nur noch zu beweisen, daß $f(x_1, x_2, x_3)$ unendlich viele Primzahlen darstellt.

$f((x))$ ist nicht das Produkt von zwei Linearformen, weil nach **1** die Determinante von $f((x))$ nicht verschwindet. Die adjungierte Form $g((y))$ von $f((x))$ ist aus diesem Grunde nicht das Quadrat einer Linearform, und nach einem bekannten Hilfssatze aus der Theorie der quadratischen Formen stellt sie nach einer ungeraden, nicht die Determinante von $f((x))$ bzw. $g((y))$ teilenden Primzahl p sowohl quadratische Reste wie Nichtreste dar.

Es darf ohne Beschränkung der Allgemeinheit angenommen werden, daß

$$(g(0, 0, 1)/p) = -1$$

ist.

Weiterhin beschränkt es nicht die Allgemeingültigkeit, wenn $f(1, 0, 0)$ zu p teilerfremd angenommen wird. Nun lassen sich ganze rationale Zahlen a, b, c so bestimmen, daß $f(a, b, c)$ zu $f(1, 0, 0)$ teilerfremd ist, während $a \equiv 0 \pmod p$, $b \not\equiv 0 \pmod p$, $c \equiv 0 \pmod p$ ist. Dann ist $h(x, y) = f(x + ay, by, cy)$ eine binäre quadratische Form, deren Diskriminante kongruent $b^2 g(0, 0, 1) \bmod p$ ist; sie ist wegen der gemachten Voraussetzung $(g(0, 0, 1)/p) = -1$ kein Quadrat. Zweitens sind die Koeffizienten $h(1, 0)$ und $h(0, 1)$ teilerfremd, d. h. $h(x, y)$ ist eine primitive Form.

$h(x, y)$ ist die Normenform eines Moduls in einem quadratischen Zahlkörper. Wir benutzen die bekannte Tatsache, daß alle Moduln im quadratischen Zahlkörper umkehrbar sind [19]). Es kann mit den üblichen transzendenten Hilfsmitteln gezeigt

[19]) D. I, § 187.

werden, daß einem umkehrbaren Modul in einem Zahlkörper unendlich viele Moduln äquivalent sind, deren Normen Primzahlen sind. Demgemäß stellt $h(x, y)$ unendlich viele Primzahlen dar, und weil $h(x, y)$ durch $f((x))$ dargestellt wird, gilt dasselbe auch für $f((x))$. Damit ist der Beweis des Satzes 8 vollständig.

4. Jede Ordnung $\mathfrak{o}$ läßt sich in der Form

$$\mathfrak{o} = [1, f\mathfrak{n}]$$

schreiben, wobei $\mathfrak{n}$ ein ganzzahliger, die 1 enthaltender Modul und f eine ganze rationale Zahl ist (z. B. $f = 1, \mathfrak{n} = \mathfrak{o}$). f teilt offenbar die Diskriminante von $\mathfrak{o}$ und ist daher nach oben hin beschränkt. Soll f möglichst groß sein, so ist durch diese Festsetzung f schon eindeutig bestimmt.

Aber auch $\mathfrak{n}$ ist dadurch eindeutig bestimmt; haben wir nämlich zwei Darstellungen,

$$\mathfrak{o} = [1, f\mathfrak{n}_1] = [1, f\mathfrak{n}_2],$$

so gibt es für jede Zahl ν_1 aus $\mathfrak{n}_1$ eine ganze rationale Zahl n und eine Zahl ν_2 aus $\mathfrak{n}_2$ derart, daß $f\nu_1 = n + f\nu_2$ ist. Daraus folgt sofort $n \equiv 0 \pmod f$, und daraus $\mathfrak{n}_1 = \mathfrak{n}_2$.

$\mathfrak{n}$ ist nach Satz 1 stets in einer Ordnung enthalten. Wird f möglichst groß bestimmt, so ist jede $\mathfrak{n}$ enthaltende Ordnung primitiv. Denn dann gibt es nicht eine ganze rationale Zahl $f' > 1$ und einen ganzzahligen Modul $\mathfrak{n}'$ so, daß $\mathfrak{n} = [1, f'\mathfrak{n}']$ ist. Nach Satz 8 enthält jetzt $\mathfrak{n}$ die Maximalordnung eines quadratischen Zahlkörpers, die erst recht in jeder $\mathfrak{n}$ enthaltenden Ordnung enthalten ist.

5. Das Hauptproblem dieses dritten Abschnittes ist die Bestimmung der Maximalordnungen, welche eine gegebene nichtmaximale Ordnung enthalten. Wegen der letzten Bemerkung in **4** wird durch den folgenden Satz dies Problem auf das Teilproblem für primitive Ordnungen reduziert:

Satz 9. *Es sei* $\mathfrak{o} = [1, f\mathfrak{n}]$ *eine Ordnung,* f *eine ganze rationale Zahl und* $\mathfrak{n}$ *ein ganzzahliger die* 1 *enthaltender Modul.* $\mathfrak{o}_1$ *sei die kleinste* $\mathfrak{n}$ *enthaltende Ordnung und* $\mathfrak{J}^{(1)}, \mathfrak{J}^{(2)}, \ldots, \mathfrak{J}^{(h)}$ *alle* $\mathfrak{o}_1$ *enthaltenden Maximalordnungen. Dann ist* $\mathfrak{o}$ *in den und nur den Maximalordnungen enthalten, welche eins der Ideale* $f\mathfrak{J}^{(1)}, f\mathfrak{J}^{(2)}, \ldots, f\mathfrak{J}^{(h)}$ *enthalten.*

Zusatz zu Satz 9. Die Maximalordnungen $\mathfrak{J}$, welche die $f\mathfrak{J}^{(i)}$ enthalten, erkennt man leicht als diejenigen, für die die Distanzideale $(\mathfrak{J} \times \mathfrak{J}^{(i)})^{-1}$ Linksteiler von $f\mathfrak{J}^{(i)}$ sind.

Beweis. Enthält die Maximalordnung $\mathfrak{J}$ eins der Ideale $f\mathfrak{J}^{(1)}, f\mathfrak{J}^{(2)}, \ldots, f\mathfrak{J}^{(h)}$, so enthält $\mathfrak{J}$ offenbar auch $\mathfrak{o}$.

Es bleibt also folgendes zu beweisen: Ist $\mathfrak{J}$ eine $\mathfrak{o}$ enthaltende Maximalordnung, so gilt für mindestens eine der Maximalordnungen $\mathfrak{J}^{(1)}, \ldots, \mathfrak{J}^{(h)}$, daß $f\mathfrak{J}^{(i)} < \mathfrak{J}$ ist.

Zum Beweise setzen wir $\mathfrak{J} = \mathfrak{J}_0$, und für $n = 1, 2, \ldots$ sei $\mathfrak{J}_{2n}$ die Rechtsordnung des Ideals $\mathfrak{J}_{2n-1} \times \mathfrak{n}$ und $\mathfrak{J}_{2n+1}$ die Linksordnung des Ideals $\mathfrak{n} \times \mathfrak{J}_{2n}$:

$$\mathfrak{J}_{2n-1} \times \mathfrak{n} = \mathfrak{J}_{2n-1} \times \mathfrak{n} \times \mathfrak{J}_{2n},$$
$$\mathfrak{n} \times \mathfrak{J}_{2n} = \mathfrak{J}_{2n+1} \times \mathfrak{n} \times \mathfrak{J}_{2n}.$$

Dann ist

$$(30)\quad \begin{aligned} \mathfrak{n} \times \mathfrak{J} = \mathfrak{n} \times \mathfrak{J}_0 &= \mathfrak{J}_1 \times \mathfrak{J}_3 \times \cdots \times \mathfrak{J}_{2n+1} \times \mathfrak{n} \times \mathfrak{J}_{2n} \times \cdots \times \mathfrak{J}_2 \times \mathfrak{J}_0 \\ &= (\mathfrak{J}_1 \times \mathfrak{J}_3) \times (\mathfrak{J}_3 \times \mathfrak{J}_5) \times \cdots \times (\mathfrak{J}_{2n+1} \times \mathfrak{n} \times \mathfrak{J}_{2n}) \times \cdots \times (\mathfrak{J}_2 \times \mathfrak{J}_0). \end{aligned}$$

Normenbildung ergibt daraus

$$(31)\quad n(\mathfrak{n} \times \mathfrak{J}_0) = \frac{n(\mathfrak{J}_{2n+1} \times \mathfrak{n} \times \mathfrak{J}_{2n})}{n((\mathfrak{J}_1 \times \mathfrak{J}_3)^{-1}) \cdots n((\mathfrak{J}_{2n-1} \times \mathfrak{J}_{2n+1})^{-1})\, n((\mathfrak{J}_{2n} \times \mathfrak{J}_{2n-2})^{-1}) \cdots n((\mathfrak{J}_2 \times \mathfrak{J}_0)^{-1})}.$$

Aus der Voraussetzung, daß $\mathfrak{o}$ in $\mathfrak{J}_0$ enthalten sein sollte, folgt nun $f\mathfrak{n} < \mathfrak{J}_0$, also ist $f\mathfrak{n} \times \mathfrak{J}_0$ ein ganzes Ideal; wegen (30) ergibt sich deshalb

$$f\mathfrak{J}_n < \mathfrak{J}_0 = \mathfrak{J} \qquad (n = 1, 2, \ldots). \tag{32}$$

Dieser Beziehung (32) können nur endlich viele verschiedene Maximalordnungen genügen, deshalb wird für alle n die Norm des Ideals $\mathfrak{J}_{2n+1} \times \mathfrak{n} \times \mathfrak{J}_{2n}$ zwischen festen Schranken liegen. Wegen (31) liegt dann auch das Produkt

$$n((\mathfrak{J}_1 \times \mathfrak{J}_3)^{-1}) \cdots n((\mathfrak{J}_{2n-1} \times \mathfrak{J}_{2n+1})^{-1})\, n((\mathfrak{J}_{2n} \times \mathfrak{J}_{2n-2})^{-1}) \cdots n((\mathfrak{J}_2 \times \mathfrak{J}_0)^{-1})$$

zwischen festen Schranken, und weil dessen sämtliche Faktoren ganz sind, ist von einem gewissen n ab

$$1 = n((\mathfrak{J}_{2n+1} \times \mathfrak{J}_{2n+3})^{-1}) = n((\mathfrak{J}_{2n+3} \times \mathfrak{J}_{2n+5})^{-1}) = \cdots$$
$$1 = n((\mathfrak{J}_{2n} \times \mathfrak{J}_{2n+2})^{-1}) = n((\mathfrak{J}_{2n+2} \times \mathfrak{J}_{2n+4})^{-1}) = \cdots.$$

Das bedeutet aber nichts anderes, als daß von diesem n ab $\mathfrak{J}_{2n+1} = \mathfrak{J}_{2n+3} = \mathfrak{J}_{2n+5} = \cdots$ und $\mathfrak{J}_{2n} = \mathfrak{J}_{2n+2} = \mathfrak{J}_{2n+4} = \cdots$ ist, d. h.

$$\mathfrak{J}_{2n+1} \times \mathfrak{n} = \mathfrak{n} \times \mathfrak{J}_{2n}. \tag{33}$$

Ich behaupte jetzt, es ist $\mathfrak{J}_{2n+1} = \mathfrak{J}_{2n}$ und $\mathfrak{J}_{2n} = \mathfrak{J}_{2n+1} > \mathfrak{n}$. Sei nämlich k die kleinste ganze rationale Zahl derart, daß $\mathfrak{n}^k$ eine Ordnung ist (vgl. § 1, 3). Dann folgt aus (33)

$$\mathfrak{J}_{2n+1} \times \mathfrak{n}^k = \mathfrak{n} \times \mathfrak{J}_{2n} \times \mathfrak{n}^{k-1}. \tag{34}$$

Deshalb stimmt die Rechtsordnung von $\mathfrak{J}_{2n+1} \times \mathfrak{n}^k$ mit der von $\mathfrak{J}_{2n} \times \mathfrak{n}^{k-1}$ überein, sie möge $\mathfrak{J}^*$ heißen. Weil $\mathfrak{n}^k$ Ordnung ist, ist $(\mathfrak{J}_{2n+1} \times \mathfrak{n}^k) \times \mathfrak{n}^k = \mathfrak{J}_{2n+1} \times \mathfrak{n}^k$, folglich

$$\mathfrak{J}^* > \mathfrak{n}^k. \tag{35}$$

Nun enthält $\mathfrak{n}^{k-1}$ wie auch $\mathfrak{n}$ die 1, und da $\mathfrak{n}^{k-1}$ ganzzahlig ist, enthält $\mathfrak{n}^{k-1}$ mit einer Zahl α auch die konjugierte $\bar{\alpha} = s(\alpha) - \alpha$. Daher ist $\overline{\mathfrak{n}^{k-1}} = \mathfrak{n}^{k-1}$ und $\overline{\mathfrak{J}_{2n} \times \mathfrak{n}^{k-1}} = \overline{\mathfrak{n}^{k-1}} \times \overline{\mathfrak{J}_{2n}} = \mathfrak{n}^{k-1} \times \mathfrak{J}_{2n}$. $\mathfrak{J}^*$ ist jetzt auch die Linksordnung von $\mathfrak{n}^{k-1} \times \mathfrak{J}_{2n}$. Eine nochmalige Anwendung von (33) ergibt $\mathfrak{n}^{k-2} \times \mathfrak{J}_{2n+1} \times \mathfrak{n} = \mathfrak{n}^{k-1} \times \mathfrak{J}_{2n}$. $\mathfrak{J}^*$ ist dann die Linksordnung von $\mathfrak{n}^{k-2} \times \mathfrak{J}_{2n+1}$. Dies Verfahren wird so fortgesetzt. Am Schluß ergibt sich $\mathfrak{J}^* = \mathfrak{J}_{2n+1}$ oder $\mathfrak{J}^* = \mathfrak{J}_{2n}$, je nachdem k gerade oder ungerade war.

Weil $\mathfrak{n}^{k-1}$ die 1 enthält, ist $\mathfrak{n} > \mathfrak{n} \times \mathfrak{n}^{k-1} = \mathfrak{n}^k$, also haben wir wegen (35) jetzt $\mathfrak{n} < \mathfrak{J}_{2n+1}$ oder $\mathfrak{n} < \mathfrak{J}_{2n}$, und weil $\mathfrak{n}$ die 1 enthält, wird (33) zu $\mathfrak{J}_{2n+1} = \mathfrak{J}_{2n}$.

$\mathfrak{J}_{2n}$ enthält als Ordnung natürlich auch die kleinste $\mathfrak{n}$ enthaltende Ordnung $\mathfrak{o}_1$, d. h. $\mathfrak{J}_{2n}$ ist eine der Ordnungen $\mathfrak{J}^{(1)}, \mathfrak{J}^{(2)}, \ldots, \mathfrak{J}^{(h)}$, und weil (32) auch gilt, wenn darin n durch $2n$ ersetzt wird, ist nunmehr Satz 9 bewiesen.

§ 6. Das Symbol $(\mathfrak{o}/p)$.

1. Nach dem in der Einleitung angegebenen Programm kommen wir jetzt dazu, das Restklassensystem einer Ordnung $\mathfrak{o}$ nach dem Modul $p\mathfrak{o}$ zu betrachten, wobei p irgendeine Primzahl ist. Es ist ein hyperkomplexes System $\mathfrak{S}_p$ über dem Körper $\mathfrak{R}_p$ der Restklassen der ganzen rationalen Zahlen mod p. $\mathfrak{N}_p$ soll stets das Radikal von $\mathfrak{S}_p$ bezeichnen.

Eine Zahl α aus $\mathfrak{o}$ definiert eindeutig eine Restklasse in $\mathfrak{S}_p$, welche ebenfalls, sobald keine Mißverständnisse zu befürchten sind, mit α bezeichnet werden soll; diese Abkürzung

hat viel für sich, da eine Basis $\varrho_0, \varrho_1, \varrho_2, \varrho_3$ von $\mathfrak{o}$ gleichzeitig als Basis von $\mathfrak{S}_p$ in bezug auf $\mathfrak{R}_p$ aufgefaßt werden kann.

Sind α und β zwei Zahlen aus $\mathfrak{o}$, und ist $\alpha \equiv \beta \pmod{p\mathfrak{o}}$, so ist auch $\bar{\alpha} \equiv \bar{\beta} \pmod{p\mathfrak{o}}$; dadurch ist in $\mathfrak{S}_p$ jeder Größe eine konjugierte eineindeutig zugeordnet. Ersetzt man in $\mathfrak{S}_p$ alle Größen durch die konjugierten, so geht dadurch $\mathfrak{N}_p$ in sich selber über; es kann daher sogar jeder Größe der Differenzalgebra $\mathfrak{S}_p - \mathfrak{N}_p$ eine konjugierte in eineindeutiger Weise zugeordnet werden. Sind α, β zwei Größen aus $\mathfrak{S}_p$ bzw. $\mathfrak{S}_p - \mathfrak{N}_p$, $\bar{\alpha}, \bar{\beta}$ die konjugierten, so ist $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$, $\overline{\alpha\beta} = \bar{\beta}\,\bar{\alpha}$.

$\mathfrak{S}_p - \mathfrak{N}_p$ enthält einen zu $\mathfrak{R}_p$ isomorphen Körper $\mathfrak{R}'_p$.

$\mathfrak{R}_p$ wie $\mathfrak{R}'_p$ bestehen aus den Summen $1 + 1 + \cdots + 1$, und können auch dadurch charakterisiert werden, daß $\alpha = \bar{\alpha}$ einzig für die Größen α aus $\mathfrak{R}_p$ bzw. $\mathfrak{R}'_p$ gilt. Jede Größe α aus $\mathfrak{S}_p$ bzw. $\mathfrak{S}_p - \mathfrak{N}_p$ genügt in $\mathfrak{R}_p$ bzw. $\mathfrak{R}'_p$ der quadratischen Gleichung $(x - \alpha)(x - \bar{\alpha}) = x^2 - s(\alpha)\,x + n(\alpha)$.

Ist p zur Diskriminante von $\mathfrak{o}$ teilerfremd, so ist $\mathfrak{N}_p = 0$, und $\mathfrak{S}_p$ ist das System der Matrizen zweiten Grades über $\mathfrak{R}_p$. Dieser Fall verdient kein weiteres Interesse.

Wenn aber p die Diskriminante von $\mathfrak{o}$ teilt, kann $\mathfrak{N}_p$ den Rang 2 oder 3 haben. Der Fall, daß $\mathfrak{N}_p$ den Rang 1 hat, tritt nicht ein. Denn dann hätte $\mathfrak{S}_p - \mathfrak{N}_p$ den Rang 3, und da es vom Rang 3 nur kommutative halbeinfache Systeme gibt, ist $\mathfrak{S}_p - \mathfrak{N}_p$ kommutativ, also direkte Summe von 1, 2 oder 3 Körpern.

Wäre $\mathfrak{S}_p - \mathfrak{N}_p$ ein Körper, so hätte $\mathfrak{S}_p - \mathfrak{N}_p$ auch den Grad 3 über $\mathfrak{R}'_p$, das widerspricht aber der Tatsache, daß alle Größen von $\mathfrak{S}_p - \mathfrak{N}_p$ in $\mathfrak{R}_p$ einer quadratischen Gleichung genügen.

Wäre $\mathfrak{S}_p - \mathfrak{N}_p$ Summe zweier Körper, so wäre in $\mathfrak{S}_p - \mathfrak{N}_p$ die 1 Summe zweier orthogonaler primitiver Idempotente, etwa $1 = \varepsilon_1 + \varepsilon_2$. Es ist dann aber auch $1 = \bar{\varepsilon}_1 + \bar{\varepsilon}_2$, wo $\bar{\varepsilon}_1, \bar{\varepsilon}_2$ wieder orthogonale Idempotente sind, und wegen der Eindeutigkeit der Zerlegung der 1 also $\bar{\varepsilon}_1 = \varepsilon_1$ oder $\bar{\varepsilon}_1 = \varepsilon_2$. Im ersten Falle zeigt sich ε_1 als eine Größe aus $\mathfrak{R}'_p$, d. h. $\varepsilon_1 = 1 + \cdots + 1$, das ist ein Widerspruch. Im zweiten Falle folgt dann noch $\bar{\varepsilon}_2 = \varepsilon_1$. Es gibt nun aber noch eine Größe α in $\mathfrak{S}_p - \mathfrak{N}_p$ so, daß $\varepsilon_1, \varepsilon_2, \alpha$ nicht linear abhängig in bezug auf $\mathfrak{R}'_p$ sind. Daher ist $[\varepsilon_1, \varepsilon_2, \alpha]$ eine Basis von $\mathfrak{S}_p - \mathfrak{N}_p$. Weil $\mathfrak{S}_p - \mathfrak{N}_p$ die direkte Summe $\mathfrak{S}_p - \mathfrak{N}_p = \varepsilon_1(\mathfrak{S}_p - \mathfrak{N}_p) + \varepsilon_2(\mathfrak{S}_p - \mathfrak{N}_p)$ ist, kann α ohne Beschränkung der Allgemeinheit so angenommen werden, daß $\varepsilon_1\alpha = 0$, $\varepsilon_2\alpha = \alpha$ ist. $\mathfrak{S}_p - \mathfrak{N}_p$ enthält auch die zu α konjugierte Größe $\bar{\alpha}$, und diese läßt sich in der Form $\bar{\alpha} = r_1\varepsilon_1 + r_2\varepsilon_2 + r_3\alpha$ mit r_1, r_2, r_3 aus $\mathfrak{R}'_p$ darstellen. Multiplikation mit ε_2 gibt jetzt $\varepsilon_2\bar{\alpha} = \overline{\alpha\varepsilon_1} = 0 = r_2\varepsilon_2 + r_3\alpha$. Weil $\varepsilon_1, \varepsilon_2, \alpha$ linear unabhängig sind, muß $r_2 = r_3 = 0$ sein, d. h. $\bar{\alpha} = r_1\varepsilon_1$, $\alpha = r_1\varepsilon_2$, und das widerspricht ebenfalls der Unabhängigkeit von $\varepsilon_1, \varepsilon_2, \alpha$.

Schließlich nehmen wir an, $\mathfrak{S}_p - \mathfrak{N}_p$ sei direkte Summe von drei Körpern, und $1 = \varepsilon_1 + \varepsilon_2 + \varepsilon_3$ sei die Zerlegung von 1 in primitive orthogonale Idempotente. Wieder gilt auch $1 = \bar{\varepsilon}_1 + \bar{\varepsilon}_2 + \bar{\varepsilon}_3$, also entweder $\bar{\varepsilon}_1 = \varepsilon_1$ oder $\bar{\varepsilon}_1 = \varepsilon_2$, $\bar{\varepsilon}_2 = \varepsilon_1$, $\bar{\varepsilon}_3 = \varepsilon_3$ oder $\bar{\varepsilon}_1 = \varepsilon_3$, $\bar{\varepsilon}_3 = \varepsilon_1$, $\bar{\varepsilon}_2 = \varepsilon_2$. Dann ist $\varepsilon_1, \varepsilon_3$ oder ε_2 in $\mathfrak{R}'_p$, und daher eine Summe $1 + 1 + \cdots + 1$, das ist ein Widerspruch.

Der Fall, daß $\mathfrak{N}_p$ den Rang 1 hat, führt also auf einen Widerspruch.

2. Im Falle, daß p in der Diskriminante von $\mathfrak{o}$ aufgeht, sind nun die folgenden drei Fälle zu unterscheiden:

1) $\mathfrak{N}_p$ hat den Rang 3, dann schreiben wir $(\mathfrak{o}/p) = 0$.
2) $\mathfrak{N}_p$ hat den Rang 2, $\mathfrak{S}_p - \mathfrak{N}_p$ ist nicht einfach, dann schreiben wir $(\mathfrak{o}/p) = 1$.
3) $\mathfrak{N}_p$ hat den Rang 2, $\mathfrak{S}_p - \mathfrak{N}_p$ ist einfach, dann schreiben wir $(\mathfrak{o}/p) = -1$.

Die Berechnung des Symbols $(\mathfrak{o}/p)$ geschieht in sehr einfacher Weise durch den

Satz 10. *Ist* $(\mathfrak{o}/p) = 0$, *so ist für jede Zahl* ϱ *aus* $\mathfrak{o}$ $(\Delta(\varrho)/p) = 0$ (Legendresymbol).

Ist $(\mathfrak{o}/p) = 1$, *so ist für jede Zahl* ϱ *in* $\mathfrak{o}$ $(\Delta(\varrho)/p) \neq -1$, *und es gibt mindestens eine mit* $(\Delta(\varrho)/p) = 1$.

Ist $(\mathfrak{o}/p) = -1$, *so ist für jede Zahl* ϱ *in* $\mathfrak{o}$ $(\Delta(\varrho)/p) \neq 1$, *und es gibt mindestens eine mit* $(\Delta(\varrho)/p) = -1$.

(Das Legendresymbol $(m/2)$ wird wie üblich definiert: $(m/2) = 0$ für gerades m; $(m/2) = 1$, wenn $m \equiv 1 \pmod 8$ ist, $(m/2) = -1$, wenn $m \equiv 5 \pmod 8$ ist.)

Beweis. Ist $(\mathfrak{o}/p) = 0$, so hat jede Größe ϱ aus $\mathfrak{S}_p$ die Gestalt $\varrho = r + \nu$, wobei r in $\mathfrak{R}_p$, ν in $\mathfrak{N}_p$ liegt. Es ist daher $s(\varrho) = 2r$, $n(\varrho) = r^2$, $\Delta(\varrho) = 0$; also gilt $\Delta(\varrho) \equiv 0 \pmod p$ für jede Größe ϱ aus $\mathfrak{o}$.

Ist $(\mathfrak{o}/p) = 1$, so ist $1 = \varepsilon_1 + \varepsilon_2$ in $\mathfrak{S}_p - \mathfrak{N}_p$, wobei $\varepsilon_1^2 = \varepsilon_1$, $\varepsilon_2^2 = \varepsilon_2$, $\varepsilon_1\varepsilon_2 = \varepsilon_2\varepsilon_1 = 0$ ist. Daraus folgt $s(\varepsilon_1) = s(\varepsilon_2) = 1$, $n(\varepsilon_1) = n(\varepsilon_2) = 0$, $n(\varepsilon_1, \varepsilon_2) = 1$. Also insbesondere $\Delta(\varepsilon_1) = 1$. Entsprechend enthält $\mathfrak{o}$ eine Zahl ε mit $\Delta(\varepsilon) \equiv 1 \pmod p$, also $(\Delta(\varepsilon)/p) = 1$. Ist α irgendeine Zahl aus $\mathfrak{o}$, so hat die durch α in $\mathfrak{S}_p - \mathfrak{N}_p$ erzeugte Restklasse die Gestalt $\varepsilon_1 r_1 + \varepsilon_2 r_2$, wobei r_1 und r_2 Größen aus $\mathfrak{R}_p'$ sind. Infolgedessen gilt nun $\Delta(\alpha) \equiv (r_1 - r_2)^2 \pmod p$, also $(\Delta(\alpha)/p) \neq -1$.

Ist schließlich $(\mathfrak{o}/p) = -1$, so ist $\mathfrak{S}_p - \mathfrak{N}_p$ ein Körper zweiten Grades über $\mathfrak{R}_p'$. Daher ist für jede Zahl ϱ aus $\mathfrak{o}$ das Symbol $(\Delta(\varrho)/p) = 0$ oder $= -1$, je nachdem die durch ϱ in $\mathfrak{S}_p$ erzeugte Restklasse zu $\mathfrak{R}_p'$ gehört oder nicht.

3. Es sei $\mathfrak{o}$ eine primitive nichtmaximale Ordnung. Wir stellen nun die Frage, in welcher Weise sich $\mathfrak{o}$ zu einer umfassenderen Ordnung erweitern läßt. Von besonderer Wichtigkeit ist dafür die Kenntnis der kleinsten von $\mathfrak{o}$ verschiedenen Ordnungen, die $\mathfrak{o}$ umfassen.

Es sei $\mathfrak{o}'$ irgendeine $\mathfrak{o}$ umfassende Ordnung und p eine in $\frac{|\mathfrak{o}|}{|\mathfrak{o}'|}$ aufgehende Primzahl. Es gibt eine Basis $1, \varrho_1', \varrho_2', \varrho_3'$ von $\mathfrak{o}'$ so, daß $\mathfrak{o} = [1, r_1\varrho_1', r_2\varrho_2', r_3\varrho_3']$ ist, wobei $r_1, r_2, r_3, \frac{r_3}{r_1}, \frac{r_2}{r_1}$ ganze rationale Zahlen sind (Elementarteilersatz!). Es ist $r_1r_2r_3 = \frac{|\mathfrak{o}|}{|\mathfrak{o}'|}$, also geht p in r_3 auf. Nun ist $\mathfrak{o}_1' = \left[\mathfrak{o}, \mathfrak{o}\frac{r_3}{p}\varrho_3'\right]$ eine von $\mathfrak{o}$ verschiedene $\mathfrak{o}$ umfassende Ordnung, für die $p\mathfrak{o}' < \mathfrak{o}$ gilt.

War $\mathfrak{o}'$ eine kleinste $\mathfrak{o}$ enthaltende Ordnung, so ist jetzt $\mathfrak{o}_1' = \mathfrak{o}'$, und wegen $p\mathfrak{o}' < \mathfrak{o}$ ist $\frac{|\mathfrak{o}|}{|\mathfrak{o}'|}$ eine Potenz von p. Weil nach Voraussetzung $\mathfrak{o}$ primitiv ist, ist $r_1 = 1$ nach Satz 8. r_2 und r_3 sind Potenzen von p, und wegen $p\mathfrak{o}_1 < \mathfrak{o}$ kann r_3 nur gleich p sein, daher kommen nur die Fälle $\mathfrak{o} = [1, \varrho_1', p\varrho_2', p\varrho_3']$, $\mathfrak{o} = [1, \varrho_1', \varrho_2', p\varrho_3']$ in Frage.

Wir wollen $\mathfrak{o}_1'$ eine *Erweiterungsordnung von* $\mathfrak{o}$ *zu* p nennen. Aus der obigen Betrachtung sieht man folgenden Hilfssatz ein: Ist $\mathfrak{o}'$ eine $\mathfrak{o}$ enthaltende Ordnung und p eine $\frac{|\mathfrak{o}|}{|\mathfrak{o}'|}$ teilende Primzahl, so gibt es zwischen $\mathfrak{o}$ und $\mathfrak{o}'$ eine Erweiterungsordnung von $\mathfrak{o}$ zu p.

4. Man kann manchmal allein aus der Struktur von $\mathfrak{S}_p$ auf die Existenz von Erweiterungsordnungen schließen:

Satz 11. *Ist* $\mathfrak{o}$ *eine primitive Ordnung und* $(\mathfrak{o}/p) \neq -1$, *so gibt es eine Erweiterungsordnung* $\mathfrak{o}_1$ *von* $\mathfrak{o}$ *zu* p, *und es ist* $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|} = p$.

Beweis. Es sei $(\mathfrak{o}/p) = 0$. $1, \varrho_1, \varrho_2, \varrho_3$ sei eine Basis für $\mathfrak{o}$ bzw. $\mathfrak{S}_p$, dabei sei $\mathfrak{R}_p = [\varrho_1, \varrho_2, \varrho_3]$. Jetzt ist $\mathfrak{m} = [p, \varrho_1, \varrho_2, \varrho_3]$ ein ganzer Modul mit durch p teilbarer Norm. $\mathfrak{m}$ ist eigentlich primitiv, denn wäre $\frac{1}{n}\mathfrak{m}$ ganzzahlig, so wäre $\mathfrak{o} = \left[1, n\frac{1}{n}\mathfrak{m}\right]$, was nach Satz 8 der Primitivität von $\mathfrak{o}$ widersprechen würde. Nach § 2, **6** ist nun $n(\mathfrak{m})$ die kleinste ganze rationale in $\mathfrak{m}$ enthaltene Zahl, d. h. es ist $n(\mathfrak{m}) = p$.

Die Linksordnung $\mathfrak{o}_1$ von $\mathfrak{m}$ enthält $\mathfrak{o}$, es ist daher auch $\mathfrak{o}_1$ primitiv; nach Satz 6 ist $\tilde{\mathfrak{o}}_1$ umkehrbar, weil es nach Satz 8 nicht einmal einen ganzzahligen Modul $\mathfrak{n}$ und eine ganze rationale Zahl $f > 1$ so gibt, daß $\mathfrak{o}_1 = [1, f\mathfrak{n}]$ wäre. Es gilt nun der Satz: Ist das Komplement der Linksordnung eines Moduls umkehrbar, so ist dieser Modul selber umkehrbar [20]); nach diesem Satz ist $\mathfrak{m}$ umkehrbar, und nach Satz 4 ist $|\mathfrak{m}| = |\mathfrak{o}_1|\, n(\mathfrak{m})^2 = |\mathfrak{o}_1|\, p^2$. Andererseits ist aber $|\mathfrak{m}| = p\,|\mathfrak{o}|$, folglich $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|} = p$. $\mathfrak{o}_1$ ist eine Erweiterungsordnung zu p.

Entsprechend kann eine Erweiterungsordnung zu p nachgewiesen werden, wenn $(\mathfrak{o}/p) = 1$ ist. Dazu sei $1, \varrho_1, \varrho_2, \varrho_3$ wieder eine Basis von $\mathfrak{o}$ bzw. $\mathfrak{S}_p$ und $\mathfrak{R}_p = [\varrho_2, \varrho_3]$. Wegen $(\Delta(\varrho_1)/p) \neq -1$ kann man eine ganze rationale Zahl x so finden, daß $n(x + \varrho_1) \equiv 0 \pmod{p}$ ist. Dann ist $\mathfrak{m} = [p, x + \varrho_1, \varrho_2, \varrho_3]$ ein ganzer Modul, von dem wie oben nachgewiesen werden kann, daß seine Linksordnung $\mathfrak{o}_1$ die Ordnung $\mathfrak{o}$ enthält, und daß $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|} = p$ gilt.

5. Das Hauptresultat der nun folgenden Untersuchungen ist der grundlegende

Satz 12. *$\mathfrak{o}$ sei eine primitive Ordnung und p eine $|\mathfrak{o}|$ teilende Primzahl.*

Ist $(\mathfrak{o}/p) = 0$, *so gibt es eine und nur eine Erweiterungsordnung* $\mathfrak{o}_1$ *von* $\mathfrak{o}$ *zu* p, *es ist* $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|} = p$.

Ist $(\mathfrak{o}/p) = 1$, *so gibt es genau zwei Erweiterungsordnungen* $\mathfrak{o}_1$ *und* $\mathfrak{o}_2$ *zu* p, *es ist* $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|} = \frac{|\mathfrak{o}|}{|\mathfrak{o}_2|} = p$.

Ist $(\mathfrak{o}/p) = -1$, *so gibt es eine und nur eine Erweiterungsordnung* $\mathfrak{o}_1$ *zu* p, *es ist* $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|} = p^2$.

Beweis. Wir beginnen mit der Diskussion des Falles, daß $\mathfrak{o}_1$ eine Erweiterungsordnung von $\mathfrak{o}$ zu p ist, für welche $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|} = p^2$ ist. Es gilt jetzt, $(\mathfrak{o}/p) = -1$ zu zeigen. Nach **3** gibt es eine Basis $1, \varrho_1, \varrho_2, \varrho_3$ für $\mathfrak{o}_1$ so, daß $\mathfrak{o} = [1, \varrho_1, p\varrho_2, p\varrho_3]$ ist. Ich behaupte, es ist $(\Delta(\varrho_1)/p) = -1$, dann folgt $(\mathfrak{o}/p) = -1$ aus Satz 10. Zum Beweise werde im Gegenteil angenommen, daß $(\Delta(\varrho_1)/p) \neq -1$ ist. Man setze

$$\begin{aligned}
\varrho_1 \cdot 1 &= \varrho_1 \cdot 1 \\
\varrho_1 \cdot \varrho_1 &= -n(\varrho_1) + \varrho_1 \cdot s(\varrho_1) \\
\varrho_1 \cdot \varrho_2 &= a_0 + \varrho_1 \cdot a_1 + \varrho_2 \cdot a_2 + \varrho_3 \cdot a_3 \\
\varrho_1 \cdot \varrho_3 &= b_0 + \varrho_1 \cdot b_1 + \varrho_2 \cdot b_2 + \varrho_3 \cdot b_3.
\end{aligned}$$

Dann ist die Matrix

$$\begin{Vmatrix} 0 & 1 & 0 & 0 \\ -n(\varrho_1) & s(\varrho_1) & 0 & 0 \\ a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{Vmatrix}$$

[20]) B. II.

dem Element ϱ_1 in derjenigen Darstellung des Systems zugeordnet, die zu dem Darstellungsmodul $\mathfrak{o}_1$ gehört. Daraus folgt $n(\varrho_1) = a_2 b_3 - a_3 b_2$, $s(\varrho_1) = a_2 + b_3$, und hieraus wiederum, daß die quadratische Form $a_3 x^2 + (b_3 - a_2)\, xy - b_2 y^2$ gleich $\Delta(\varrho_1)$ ist. Weil nun $\Delta(\varrho_1)$ nach p nicht quadratischer Nichtrest sein sollte, gibt es zwei teilerfremde ganze rationale Zahlen m, n so, daß $a_3 m^2 + (b_3 - a_2)\, mn - b_2 n^2 \equiv 0 \pmod{p}$ ist. Wählt man zwei weitere ganze rationale Zahlen m', n', für welche $mn' - nm' = 1$ gilt, und setzt man

$$\varrho_2' = m\,\varrho_2 + n\,\varrho_3,$$
$$\varrho_3' = m'\varrho_2 + n'\varrho_3,$$

so wird $\mathfrak{o}_1' = [1, \varrho_1, \varrho_2', p\varrho_3']$ eine $\mathfrak{o}$ enthaltende, in $\mathfrak{o}_1$ enthaltene Ordnung; sie ist von $\mathfrak{o}$ und $\mathfrak{o}_1$ verschieden, und das widerspricht der vorausgesetzten Minimaleigenschaft von $\mathfrak{o}_1$. Also muß wirklich $(\Delta(\varrho_1)/p) = -1$ sein.

Es kann aber auch gleich gezeigt werden, daß in diesem Falle $\mathfrak{o}_1$ die einzige Erweiterungsordnung von $\mathfrak{o}$ zu p ist. Das ergibt sich sofort aus der Tatsache, daß jede Zahl ϱ, für welche $p\varrho < \mathfrak{o}$ ist, in $\mathfrak{o}_1$ liegt; und dies sieht man so ein: es sei $p\varrho = r_0 + r_1\varrho_1 + r_2 p\varrho_2 + r_3 p\varrho_3$ mit ganzen rationalen r_0, r_1, r_2, r_3; dann gelten die Kongruenzen

$$s(p\varrho) \equiv 2r_0 + r_1 s(\varrho_1) \equiv 0 \pmod{p},$$
$$n(p\varrho) \equiv r_0^2 + r_0 r_1 s(\varrho_1) + r_1^2 n(\varrho_1) \equiv 0 \pmod{p},$$
$$\Delta(p\varrho) \equiv r_1^2 \Delta(\varrho_1) \equiv 0 \pmod{p}.$$

Wegen $(\Delta(\varrho_1)/p) = -1$ folgt aus der letzten Kongruenz $r_1 \equiv 0 \pmod{p}$. Folglich muß auch $r_0 \equiv 0 \pmod{p}$ sein, und aus diesem Grunde liegt ϱ in $\mathfrak{o}_1$, wie behauptet wurde.

6. Nun sei $\mathfrak{o}_1$ eine Erweiterungsordnung von $\mathfrak{o}$ zu p und $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|} = p$. Da $\mathfrak{o}$ und $\mathfrak{o}_1$ primitiv sind, sind nach Satz 6, wie schon oben (in **4**) geschlossen wurde, $\tilde{\mathfrak{o}}$ und $\tilde{\mathfrak{o}}_1$ umkehrbar; und nach § 4, **2** ist $\mathfrak{o}_1 \backslash \mathfrak{o}$ ein umkehrbarer Modul der Norm $n(\mathfrak{o}_1 \backslash \mathfrak{o}) = \frac{|\mathfrak{o}|}{|\mathfrak{o}_1|} = p$. Deswegen ist $\mathfrak{o}_1 \backslash \mathfrak{o}$ eigentlich primitiv und nach Satz 7

$$\mathfrak{o} = [1, \mathfrak{o}_1 \backslash \mathfrak{o}]. \tag{36}$$

Ist ϱ eine Zahl aus $\mathfrak{o}$, so gibt es wegen (36) eine ganze rationale Zahl r und eine Zahl π aus $\mathfrak{o}_1 \backslash \mathfrak{o}$ so, daß $\varrho = r + \pi$ ist. Wegen $n(\pi) \equiv 0 \pmod{p}$ folgt deshalb $(\Delta(\varrho)/p) \neq -1$, also ist nach Satz 10 $(\mathfrak{o}/p) \neq -1$.

$\mathfrak{o}_2$ sei eine andere Erweiterungsordnung von $\mathfrak{o}$ zu p. Nach **5** kann nicht $\frac{|\mathfrak{o}|}{|\mathfrak{o}_2|} = p^2$ sein, denn dann wäre $(\mathfrak{o}/p) = -1$, also ist $\frac{|\mathfrak{o}|}{|\mathfrak{o}_2|} = p$ und

$$\mathfrak{o} = [1, \mathfrak{o}_2 \backslash \mathfrak{o}]. \tag{37}$$

Aus (36) und (37) ergibt sich $\mathfrak{o}_2 \backslash \mathfrak{o} = \mathfrak{o}_1 \backslash \mathfrak{o}$ oder $\mathfrak{o}_2 \backslash \mathfrak{o} = \mathfrak{o}/\mathfrak{o}_1 = \overline{\mathfrak{o}_1 \backslash \mathfrak{o}}$. Betrachten wir nämlich das Restsystem $\mathfrak{S}_p$ von $\mathfrak{o}$ nach $p\mathfrak{o}$! Falls $\mathfrak{N}_p$ den Rang 3 über $\mathfrak{R}_p$ hat, ist $\mathfrak{N}_p \equiv \mathfrak{o}_1 \backslash \mathfrak{o} \equiv \mathfrak{o}_2 \backslash \mathfrak{o} \pmod{p\mathfrak{o}}$, und weil $\mathfrak{o}_1 \backslash \mathfrak{o}$ und $\mathfrak{o}_2 \backslash \mathfrak{o}$ als ganze primitive Moduln nach § 2, **6** ihre Norm p enthalten, ist $\mathfrak{o}_1 \backslash \mathfrak{o} = \mathfrak{o}_2 \backslash \mathfrak{o}$. Hat aber $\mathfrak{N}_p$ den Rang 2, so kann es in $\mathfrak{S}_p$ nur zwei Moduln mit verschwindender Norm geben, dieses sind gerade die Restklassensysteme von $\mathfrak{o}_1 \backslash \mathfrak{o}$ und $\overline{\mathfrak{o}_1 \backslash \mathfrak{o}}$ mod $p\mathfrak{o}$. Daher ist jetzt $\mathfrak{o}_2 \backslash \mathfrak{o} \equiv \mathfrak{o}_1 \backslash \mathfrak{o}$ oder $\mathfrak{o}_2 \backslash \mathfrak{o} \equiv \overline{\mathfrak{o}_1 \backslash \mathfrak{o}} \pmod{p\mathfrak{o}}$, woraus wie oben die Behauptung folgt.

Ist $(\mathfrak{o}/p) = 0$, so gibt es nach Obigem eine und nur eine Erweiterungsordnung zu p.

Ist aber $(\mathfrak{o}/p) = 1$, so gibt es deren höchstens zwei. Um zu zeigen, daß es genau

zwei gibt, genügt es, zu beweisen, daß die Rechtsordnung von $\mathfrak{o}_1\backslash\mathfrak{o}$ von $\mathfrak{o}_1$ verschieden ist, denn diese umfaßt auch $\mathfrak{o}$. Im Falle $(\mathfrak{o}/p) = 1$ sind nicht die Spuren aller Zahlen aus $\mathfrak{o}_1\backslash\mathfrak{o}$ durch p teilbar, denn sonst wäre wegen (36) $\mathfrak{o}_1\backslash\mathfrak{o}$, mod $p\mathfrak{o}$ betrachtet, das Radikal $\mathfrak{N}_p$ von $\mathfrak{S}_p$ und hätte über $\mathfrak{N}_p$ den Rang 3. Es sei ϱ eine Zahl aus $\mathfrak{o}_1\backslash\mathfrak{o}$ mit zu p teilerfremder Spur. ϱ' sei eine weitere Zahl aus $\mathfrak{o}_1\backslash\mathfrak{o}$, deren Restklasse mod $p\mathfrak{o}$ in $\mathfrak{N}_p$ liegt; es soll aber nicht $\frac{1}{p}\varrho'$ in $\mathfrak{o}_1$ liegen. Daß es eine solche Zahl ϱ' gibt, ersieht man daraus, daß wegen $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|} = p$ nicht $\frac{\mathfrak{N}_p}{p}$ in $\mathfrak{o}_1$ liegt.

Wäre nun $\mathfrak{o}_1$ sowohl Linksordnung wie Rechtsordnung von $\mathfrak{o}_1\backslash\mathfrak{o}$, so wäre

$$(\mathfrak{o}_1\backslash\mathfrak{o}) \times (\overline{\mathfrak{o}_1\backslash\mathfrak{o}}) = (\overline{\mathfrak{o}_1\backslash\mathfrak{o}}) \times (\mathfrak{o}_1\backslash\mathfrak{o}) = p\mathfrak{o}_1 .$$

Das ergäbe insbesondere $\varrho\bar{\varrho}' \equiv \bar{\varrho}'\varrho \equiv 0 \pmod{p\mathfrak{o}_1}$. Nun verifiziert man leicht die Beziehung

$$\varrho\bar{\varrho}' + \bar{\varrho}'\varrho - n(\varrho, \varrho') = s(\varrho')\,\varrho - s(\varrho)\,\varrho' .$$

Daraus erhält man $\varrho\bar{\varrho}' + \bar{\varrho}'\varrho - n(\varrho, \varrho') \equiv s(\varrho)\,\varrho' \equiv 0 \pmod{p\mathfrak{o}_1}$. Das aber widerspricht den Voraussetzungen, daß $s(\varrho)$ zu p teilerfremd sein und $\frac{1}{p}\varrho'$ nicht in $\mathfrak{o}_1$ liegen sollte.

Jetzt ist Satz 12 in vollem Umfange bewiesen.

Ist $\mathfrak{o}_2$ die Rechtsordnung von $\mathfrak{o}_1\backslash\mathfrak{o}$, so gilt $\mathfrak{o} \frown \mathfrak{o}_1 < \mathfrak{o}_2$. Wegen $\frac{|\mathfrak{o}|}{|\mathfrak{o}_1|} = \frac{|\mathfrak{o}|}{|\mathfrak{o}_2|} = p$ können aber zwischen $\mathfrak{o}$ und $\mathfrak{o}_1$ bzw. $\mathfrak{o}$ und $\mathfrak{o}_2$ keine Zwischenordnungen mehr liegen. Deshalb ist jetzt

$$\mathfrak{o} = \mathfrak{o}_1 \frown \mathfrak{o}_2 .$$

7. Wird eine primitive Ordnung $\mathfrak{o}$ vorgelegt, so kann man nun leicht alle Ordnungen berechnen, die $\mathfrak{o}$ enthalten.

Zunächst muß man alle in $|\mathfrak{o}|$ aufgehenden Primzahlen kennen. Ist $(\mathfrak{o}/p) \neq -1$, so ist nach Satz 11 p sicher ein Teiler von $|\mathfrak{o}|$. Ist aber $(\mathfrak{o}/p) = -1$, so ist p dann und nur dann ein Teiler von $|\mathfrak{o}|$, wenn p^2 in $d(\mathfrak{o})$ aufgeht. Denn dann sei $\mathfrak{J}$ eine $\mathfrak{o}$ enthaltende Maximalordnung und $d(\mathfrak{o}) = |\mathfrak{o}|\,d(\mathfrak{J})$. $d(\mathfrak{J})$ ist stets quadratfrei, daher geht p in $|\mathfrak{o}|$ auf, sobald p^2 in $d(\mathfrak{o})$ aufgeht. Falls aber p ein Teiler von $|\mathfrak{o}|$ ist, so teilt p^2 nach Satz 12 $|\mathfrak{o}|$, wenn $(\mathfrak{o}/p) = -1$ ist.

$p_1, p_2, \ldots, p_n$ seien alle $|\mathfrak{o}|$ teilenden Primzahlen. Jetzt berechne man alle Erweiterungsordnungen $\mathfrak{o}_1, \mathfrak{o}_2, \ldots, \mathfrak{o}_{n'}$ von $\mathfrak{o}$ zu $p_1, p_2, \ldots, p_n$ und höre erst dann mit der Fortsetzung dieses Verfahrens auf, wenn man zu Maximalordnungen gekommen ist.

Wie sich diese Rechnung im einzelnen darstellt, soll kurz mit Hilfe von Beispielen erläutert werden.

1. Fall. $(\mathfrak{o}/p) = -1 .$

Man stelle eine Basis $1, \varrho_1, \varrho_2, \varrho_3$ von $\mathfrak{o}$ bzw. $\mathfrak{S}_p$ auf, wobei $\mathfrak{N}_p = [\varrho_2, \varrho_3]$ ist. Dann ist $\mathfrak{o}_1 = \left[1, \varrho_1, \frac{1}{p}\varrho_2, \frac{1}{p}\varrho_3\right]$ die Erweiterungsordnung zu p.

Beispiel. $\iota_1, \iota_2, \iota_3$ seien die Basiseinheiten der Hamiltonschen Quaternionen, $\mathfrak{o}$ sei die Ordnung

$$\mathfrak{o} = [1, \iota_1, 3\iota_2, 3\iota_3] .$$

Es ist $|\mathfrak{o}| = 18$. Wegen $(\Delta(\iota)/3) = -1$ und Satz 10 ist $(\mathfrak{o}/3) = -1$, also ist $\mathfrak{o}_1 = [1, \iota_1, \iota_2, \iota_3]$ die einzige Erweiterungsordnung zu 3.

2. Fall. $(\mathfrak{o}/p) = 0$.

Man stelle eine Basis $1, \varrho_1, \varrho_2, \varrho_3$ für $\mathfrak{o}$ bzw. $\mathfrak{S}_p$ auf, wobei $\mathfrak{N}_p = [\varrho_1, \varrho_2, \varrho_3]$ ist. Dann ist die Linksordnung bzw. Rechtsordnung $\mathfrak{o}_1$ von $[p, \varrho_1, \varrho_2, \varrho_3]$ die Erweiterungsordnung zu p; dieser Modul ist übrigens gleich $\mathfrak{o}_1\backslash\mathfrak{o}$.

Beispiel. $\iota_1, \iota_2, \iota_3$ seien wieder die Basiseinheiten der Hamiltonschen Quaternionen und

$$\mathfrak{o} = [1, \iota_1 - \iota_2 - \iota_3,\ 3\iota_2, 3\iota_3], \qquad (\mathfrak{o}/3) = 0,$$
$$\mathfrak{o}_1\backslash\mathfrak{o} = [3, \iota_1 - \iota_2 - \iota_3, 3\iota_2, 3\iota_3], \qquad \mathfrak{o}_1 = [1, \iota_1 + \iota_2,\ \iota_1 + \iota_3,\ \iota_1 - \iota_2 - \iota_3].$$

3. Fall. $(\mathfrak{o}/p) = 1$.

Hier stelle man eine Basis $1, \varrho_1, \varrho_2, \varrho_3$ von $\mathfrak{o}$ bzw. $\mathfrak{S}_p$ auf, wobei $\mathfrak{N}_p = [\varrho_2, \varrho_3]$ ist und $n(\varrho_1) \equiv 0 \pmod p$. $\mathfrak{o}_1$ und $\mathfrak{o}_2$ sind nun Linksordnung und Rechtsordnung von $[p, \varrho_1, \varrho_2, \varrho_3]$, und dieser Modul ist gleich $\mathfrak{o}_1\backslash\mathfrak{o} = \mathfrak{o}/\mathfrak{o}_2$.

Beispiel. $\iota_1, \iota_2, \iota_3$ seien wieder die Basiseinheiten der Hamiltonschen Quaternionen und

$$\mathfrak{o} = [1, \tfrac{1}{2}(1 + \iota_1 + 5\iota_2 + 5\iota_3), 5\iota_2, 5\iota_3].$$
$$|\mathfrak{o}| = 25, \qquad (\mathfrak{o}/5) = 1.$$
$$[1, \iota_1, \iota_2 + 2\iota_3, \tfrac{1}{2}(1 + \iota_1 + 5\iota_2 + 5\iota_3)] = \mathfrak{o}_1,$$
$$[1, \iota_1, \tfrac{1}{2}(1 + \iota_1 + 5\iota_2 - 5\iota_3)] = \mathfrak{o}_2.$$

§ 7. Durchschnitte von Maximalordnungen.

1. Von besonderem Interesse ist die Frage nach der Anzahl der Maximalordnungen, welche eine gegebene nichtmaximale Ordnung enthalten; wir wollen uns bei ihrer Beantwortung auf primitive Ordnungen beschränken. Ja es genügt sogar, wie wir gleich zeigen werden, sich auf solche Ordnungen $\mathfrak{o}$ zu beschränken, für die $(\mathfrak{o}/p)$ für jede $|\mathfrak{o}|$ teilende Primzahl p gleich 1 ist.

Ist nämlich p eine in $|\mathfrak{o}|$ aufgehende Primzahl und $(\mathfrak{o}/p) \neq 1$, ist ferner $\mathfrak{J}$ irgendeine $\mathfrak{o}$ enthaltende Maximalordnung, so gibt es nach § 6, **3** zwischen $\mathfrak{J}$ und $\mathfrak{o}$ eine Erweiterungsordnung $\mathfrak{o}_1$ von $\mathfrak{o}$ zu p. Da es nach Satz 12 nur eine Erweiterungsordnung zu p gibt, liegt $\mathfrak{o}_1$ zwischen jeder $\mathfrak{o}$ enthaltenden Maximalordnung und $\mathfrak{o}$, d. h. $\mathfrak{o}_1$ ist in ebensovielen Maximalordnungen wie $\mathfrak{o}$ enthalten. Daher genügt es, die Anzahl der $\mathfrak{o}_1$ enthaltenden Maximalordnungen zu kennen. $\mathfrak{o}_1$ hat nun eine kleinere Determinante als $\mathfrak{o}$; wiederholt man die angegebene Operation genügend oft, so kommt man schließlich zu einer Ordnung $\mathfrak{o}'$, die in ebensovielen Maximalordnungen wie $\mathfrak{o}$ enthalten ist und dazu die Eigenschaft hat, daß $(\mathfrak{o}'/p) = 1$ ist für jede $|\mathfrak{o}'|$ teilende Primzahl p.

Die primitiven Ordnungen $\mathfrak{o}$, für welche alle Symbole $(\mathfrak{o}/p)$ den Wert 1 haben, sobald p eine $|\mathfrak{o}|$ teilende Primzahl ist, sind Durchschnitte von Maximalordnungen. Diese Behauptung sei schon für Ordnungen mit kleinerer Determinante als $|\mathfrak{o}|$ bewiesen; ist dann p eine $|\mathfrak{o}|$ teilende Primzahl und $\mathfrak{o}_1, \mathfrak{o}_2$ die beiden Erweiterungsordnungen zu p, so sind nach der Induktionsannahme $\mathfrak{o}_1$ und $\mathfrak{o}_2$ Durchschnitte von Maximalordnungen. Nach § 6, **6** ist aber $\mathfrak{o} = \mathfrak{o}_1 \cap \mathfrak{o}_2$, und somit ist auch $\mathfrak{o}$ Durchschnitt von Maximalordnungen.

Es gilt sogar der

Satz 13. *Eine Ordnung* $\mathfrak{o}$ *ist dann und nur dann Durchschnitt zweier Maximalordnungen, wenn* $\mathfrak{o}$ *primitiv ist und für jede* $|\mathfrak{o}|$ *teilende Primzahl* $(\mathfrak{o}/p) = 1$ *gilt.*

Der Beweis muß vorläufig zurückgestellt werden.

2. Zuerst sollen die elementaren Eigenschaften der Durchschnitte zweier Maximalordnungen abgeleitet werden.

Sind $\mathfrak{J}$ und $\mathfrak{J}'$ zwei (verschiedene) Maximalordnungen, so heißt das größte ganze Ideal, dessen Linksordnung $\mathfrak{J}$ und dessen Rechtsordnung $\mathfrak{J}'$ ist, das Distanzideal von $\mathfrak{J}$ nach $\mathfrak{J}'$, es ist gleich $(\mathfrak{J}' \times \mathfrak{J})^{-1}$ [21]).

Die Bedingung, daß das Distanzideal ganz ist und $\mathfrak{J}'$ zur Rechtsordnung hat, hat zur Folge, daß $(\mathfrak{J}' \times \mathfrak{J})^{-1}$ in $\mathfrak{J}'$ enthalten ist, daher gilt

$$\mathfrak{J}\backslash\mathfrak{J}' > (\mathfrak{J}' \times \mathfrak{J})^{-1}.$$

Nach § 4, **1** ist aber $\mathfrak{J} \times (\mathfrak{J}\backslash\mathfrak{J}') = (\mathfrak{J}\backslash\mathfrak{J}') \times \mathfrak{J}' = \mathfrak{J}\backslash\mathfrak{J}'$, also ist $\mathfrak{J}\backslash\mathfrak{J}'$ ein ganzes Ideal der Linksordnung $\mathfrak{J}$ und der Rechtsordnung $\mathfrak{J}'$, es muß daher in $(\mathfrak{J}' \times \mathfrak{J})^{-1}$ enthalten sein. Somit haben wir die Beziehung

$$\mathfrak{J}\backslash\mathfrak{J}' = (\mathfrak{J}' \times \mathfrak{J})^{-1}.$$

Ebenfalls nach § 4, **1** ist $\mathfrak{J}\backslash\mathfrak{J}' = \mathfrak{J}\backslash(\mathfrak{J} \cap \mathfrak{J}')$, und daher gilt

$$\mathfrak{J}\backslash(\mathfrak{J} \cap \mathfrak{J}') = (\mathfrak{J}' \times \mathfrak{J})^{-1}. \tag{38}$$

$(\mathfrak{J}' \times \mathfrak{J})^{-1}$ ist (eigentlich) primitiv, nach (38) und Satz 7 also

$$\mathfrak{J} \cap \mathfrak{J}' = [1, (\mathfrak{J}' \times \mathfrak{J})^{-1}]. \tag{39}$$

Wir beweisen jetzt den

Satz 14. *$\mathfrak{J}$ und $\mathfrak{J}'$ seien zwei Maximalordnungen. Alle Maximalordnungen, die den Durchschnitt $\mathfrak{J} \cap \mathfrak{J}'$ enthalten, werden durch die Rechtsordnungen der Linksteiler (bzw. die Linksordnungen der Rechtsteiler) von $(\mathfrak{J} \times \mathfrak{J}')^{-1}$ geliefert.*

Beweis. Es seien $\mathfrak{a}$, $\mathfrak{b}$ ganze Ideale und $(\mathfrak{J}' \times \mathfrak{J})^{-1} = \mathfrak{a}\mathfrak{b}$. $\mathfrak{J}^*$ sei die Rechtsordnung von $\mathfrak{a}$. Dann ist $\mathfrak{J} \cap \mathfrak{J}' = [1, (\mathfrak{J}' \times \mathfrak{J})^{-1}] < [1, \mathfrak{a}] < \mathfrak{J}^*$.

Umgekehrt sei $\mathfrak{J}^*$ eine $\mathfrak{J} \cap \mathfrak{J}'$ enthaltende Maximalordnung, dann ist

$$\mathfrak{J} \cap \mathfrak{J}' < \mathfrak{J} \cap \mathfrak{J}^* \text{ und } \mathfrak{J}\backslash(\mathfrak{J} \cap \mathfrak{J}') < \mathfrak{J}\backslash(\mathfrak{J} \cap \mathfrak{J}^*),$$

und $\mathfrak{J}\backslash(\mathfrak{J} \cap \mathfrak{J}^*) = (\mathfrak{J}^* \times \mathfrak{J})^{-1}$ ist ein Linksteiler von $\mathfrak{J}\backslash(\mathfrak{J} \cap \mathfrak{J}')$; die Rechtsordnung von $(\mathfrak{J}^* \times \mathfrak{J})^{-1}$ ist $\mathfrak{J}^*$.

Auf Grund von Satz 14 läßt sich die Anzahl der Maximalordnungen, welche einen Durchschnitt $\mathfrak{J} \cap \mathfrak{J}^*$ von Maximalordnungen enthalten, leicht abzählen. $\mathfrak{J} \cap \mathfrak{J}'$ ist in so vielen Maximalordnungen enthalten, wie $(\mathfrak{J}' \times \mathfrak{J})^{-1}$ Linksteiler besitzt, denn je zwei verschiedene Linksteiler eines Distanzideals haben bekanntlich verschiedene Rechtsordnungen [22]). $(\mathfrak{J}' \times \mathfrak{J})^{-1}$ hat so viele Linksteiler, wie $n((\mathfrak{J}' \times \mathfrak{J})^{-1})$ Teiler besitzt; denn einer Zerlegung $(\mathfrak{J}' \times \mathfrak{J})^{-1} = \mathfrak{a}\mathfrak{b}$ entspricht die Zerlegung $n((\mathfrak{J}' \times \mathfrak{J})^{-1}) = n(\mathfrak{a})\, n(\mathfrak{b})$ der Norm. Und ist $n((\mathfrak{J}' \times \mathfrak{J})^{-1}) = ab$, wobei a und b ganze rationale Zahlen sind, so ist $\mathfrak{a} = (\mathfrak{J}' \times \mathfrak{J})^{-1} + a\mathfrak{J}$ ein ganzes Ideal der Norm a, welches $(\mathfrak{J}' \times \mathfrak{J})^{-1}$ von links teilt. Ist nun $n((\mathfrak{J}' \times \mathfrak{J})^{-1}) = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ die Zerlegung von $n((\mathfrak{J}' \times \mathfrak{J})^{-1})$ in Primzahlpotenzen, so hat $n((\mathfrak{J}' \times \mathfrak{J})^{-1})$ gerade $(a_1 + 1)(a_2 + 1) \cdots (a_n + 1)$ Teiler. Schließlich beachte man, daß $(\mathfrak{J}' \times \mathfrak{J})^{-1}$ primitiv ist, und daß wegen (38) und Satz 7 $n((\mathfrak{J}' \times \mathfrak{J})^{-1}) = |\mathfrak{J} \cap \mathfrak{J}'|$ ist; dann gilt der

[21]) Bezüglich des Begriffes des Distanzideals vgl. B. I, B. II.

[22]) Ein Distanzideal besitzt nämlich keine nichttrivialen, d. h. von einer Ordnung verschiedenen, gleichseitigen Teiler. Umgekehrt ist ein ganzes Ideal ohne nichttriviale gleichseitige Teiler Distanzideal. Man kann diese Tatsache auch so formulieren: *Ein ganzes Ideal ist dann und nur dann Distanzideal, wenn es primitiv ist und seine Norm (und damit es selbst) zur Diskriminante der Algebra teilerfremd ist.* Daraus folgt, daß ein von einer Ordnung verschiedener Teiler eines Distanzideals selbst ein solches ist.

Satz 15. *Sind* $\mathfrak{J}, \mathfrak{J}'$ *Maximalordnungen und ist*

$$|\mathfrak{J} \frown \mathfrak{J}'| = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

die Zerlegung der Determinante des Durchschnitts in Primzahlpotenzen, so ist $\mathfrak{J} \frown \mathfrak{J}'$ *in* $(a_1 + 1) \cdots (a_n + 1)$ *Maximalordnungen enthalten.*

4. Wir kommen jetzt zu dem Beweis von Satz 13. Zunächst zeigen wir, daß der Durchschnitt zweier Maximalordnungen $\mathfrak{J}, \mathfrak{J}'$ eine primitive Ordnung ist.

Wäre nämlich $\mathfrak{J} \frown \mathfrak{J}'$ nicht primitiv, so gäbe es nach Satz 8 einen ganzzahligen Modul $\mathfrak{n}$ und eine ganze rationale Zahl $f > 1$ so, daß $\mathfrak{J} \frown \mathfrak{J}' = [1, f\mathfrak{n}]$ ist. $\mathfrak{n}$ ist nach Satz 1 in einer Maximalordnung $\mathfrak{J}^*$ enthalten; eine lineare Substitution, die eine Basis von $\mathfrak{J}^*$ in eine von $[1, f\mathfrak{n}]$ transformiert, ist also durch f^3 teilbar, daher ist die Determinante $|\mathfrak{J} \frown \mathfrak{J}'| = n(\mathfrak{J}\backslash(\mathfrak{J} \frown \mathfrak{J}'))$ durch f^3 teilbar.

Nach (38) und (39) hat nun jede Zahl φ aus $\mathfrak{J}\backslash(\mathfrak{J} \frown \mathfrak{J}')$ die Gestalt $\varphi = g + f\nu$, wobei g ganz und rational und ν in $\mathfrak{n}$ enthalten ist. Normbildung ergibt

$$n(\varphi) = g^2 + fgs(\nu) + f^2 n(\nu).$$

Nun ist $n(\varphi)$ durch $n(\mathfrak{J}\backslash(\mathfrak{J} \frown \mathfrak{J}'))$ und daher durch f^3 teilbar, daher muß g durch f teilbar sein und desgleichen auch φ. Da dies für alle Zahlen φ aus $\mathfrak{J}\backslash(\mathfrak{J} \frown \mathfrak{J}')$ gelten muß, kann $\mathfrak{J}\backslash(\mathfrak{J} \frown \mathfrak{J}')$ nicht primitiv sein. Das ist aber ein Widerspruch.

Ist p eine in $|\mathfrak{J} \frown \mathfrak{J}'|$ aufgehende Primzahl, so ist $(\mathfrak{J} \frown \mathfrak{J}'/p) = 1$. Wäre nämlich $(\mathfrak{J} \frown \mathfrak{J}'/p) \neq 1$, so gäbe es nach **1** eine $\mathfrak{J} \frown \mathfrak{J}'$ enthaltende Ordnung $\mathfrak{o}$ mit einer Determinante, die durch p weniger oft als $|\mathfrak{J} \frown \mathfrak{J}'|$ teilbar ist, und die in ebenso vielen Maximalordnungen wie $\mathfrak{J} \frown \mathfrak{J}'$ enthalten ist. Das widerspricht dem Satz 15, wenn $\mathfrak{o}$ Durchschnitt zweier Maximalordnungen ist. Daß dies für $\mathfrak{o}$ zutrifft, sieht man folgendermaßen ein:

Es ist

$$\mathfrak{J}\backslash\mathfrak{o} > \mathfrak{J}\backslash(\mathfrak{J} \frown \mathfrak{J}'),$$

$\mathfrak{J}\backslash\mathfrak{o}$ ist also ein Linksteiler von $\mathfrak{J}\backslash(\mathfrak{J} \frown \mathfrak{J}')$. Jeder Teiler eines Distanzideals ist aber selber ein Distanzideal [22]), also gibt es eine Maximalordnung $\mathfrak{J}^*$ so, daß $\mathfrak{J}\backslash\mathfrak{o} = (\mathfrak{J}^* \times \mathfrak{J})^{-1}$ ist. Nach Satz 7 ist nun $\mathfrak{o} = [1, \mathfrak{J}\backslash\mathfrak{o}]$ und nach (39) $\mathfrak{o} = \mathfrak{J} \frown \mathfrak{J}^*$.

Damit ist der zweite Teil des Satzes 13 bewiesen.

5. Der erste Teil des Satzes 13 kann ohne Satz 8 und ohne analytische Hilfsmittel bewiesen werden. Eine primitive Ordnung $\mathfrak{o}$, für die stets $(\mathfrak{o}/p) = 1$ gilt, wenn p eine $|\mathfrak{o}|$ teilende Primzahl ist, wird nach **1** Durchschnitt von Maximalordnungen. Der erste Teil des Satzes 13 kann nun auch so formuliert werden:

Enthalten beliebig viele Maximalordnungen $\mathfrak{J}_1, \mathfrak{J}_2, \ldots, \mathfrak{J}_n$ *die Maximalordnung* $\mathfrak{O}$ *eines quadratischen Zahlkörpers, so gibt es zwei Maximalordnungen* $\mathfrak{J}_{n+1}, \mathfrak{J}_{n+2}$ *derart, daß*

$$\mathfrak{J}_1 \frown \mathfrak{J}_2 \frown \cdots \frown \mathfrak{J}_n = \mathfrak{J}_{n+1} \frown \mathfrak{J}_{n+2}$$

ist.

$\mathfrak{O}$ ist dann natürlich auch in $\mathfrak{J}_{n+1}$ und $\mathfrak{J}_{n+2}$ enthalten, und daher genügt es, die Behauptung für den Fall $n = 3$ zu beweisen. Der Beweis führt über die Konstruktion einer Maximalordnung $\mathfrak{J}_6$ zu einer direkten Angabe von Ordnungen $\mathfrak{J}_4, \mathfrak{J}_5$, für welche $\mathfrak{J}_1 \frown \mathfrak{J}_2 \frown \mathfrak{J}_3 = \mathfrak{J}_4 \frown \mathfrak{J}_5$ gilt. Die leitende Idee ist, die Ideale des Quaternionensystems auf Ideale in $\mathfrak{O}$ abzubilden, hier eine gewisse Konstruktion auszuführen und diese schließlich rückwärts sich auf Quaternionenideale auswirken zu lassen.

Zur Abkürzung bezeichnen wir für alle vorkommenden Indizes die Distanzideale $(\mathfrak{J}_k \times \mathfrak{J}_i)^{-1}$ mit $\mathfrak{d}_{ik}$, ferner setzen wir

(40) $$\mathfrak{D}_{ik} = \mathfrak{O} \frown \mathfrak{d}_{ik}.$$

Es gilt nun der Satz [23]), *daß stets*

$$\mathfrak{d}_{ik} = \mathfrak{J}_i \times \mathfrak{D}_{ik} = \mathfrak{D}_{ik} \times \mathfrak{J}_k \tag{41}$$

ist, wenn $\mathfrak{O}$ *in* $\mathfrak{J}_i$ *und* $\mathfrak{J}_k$ *enthalten ist.* Zur Bequemlichkeit des Lesers lasse ich einen Beweis folgen. Unter den gemachten Voraussetzungen sind die $\mathfrak{D}_{ik}$ ganze Ideale in $\mathfrak{O}$. Ferner ist $[1, \mathfrak{D}_{ik}] = [1, \mathfrak{d}_{ik} \cap \mathfrak{O}] = [1, \mathfrak{d}_{ik}] \cap \mathfrak{O}$, und nach (39) $[1, \mathfrak{D}_{ik}] = \mathfrak{J}_i \cap \mathfrak{J}_k \cap \mathfrak{O} = \mathfrak{O}$; letztere Gleichung hat zur Folge, daß $n(\mathfrak{D}_{ik})$ die kleinste ganze rationale in $\mathfrak{D}_{ik}$ liegende Zahl ist. Diese ist aber nach (40) auch die kleinste ganze rationale in $\mathfrak{d}_{ik}$ liegende Zahl, und da $\mathfrak{d}_{ik}$ ein ganzes primitives Ideal ist, ist diese nach § 2, **6** auch gleich $n(\mathfrak{d}_{ik})$; d. h. es ist

$$n(\mathfrak{D}_{ik}) = n(\mathfrak{d}_{ik}). \tag{42}$$

Die Beziehung $\mathfrak{J}_i \times \mathfrak{D}_{ik} < \mathfrak{d}_{ik}$ folgt nun direkt aus $\mathfrak{O} < \mathfrak{J}_i$, und es ist

$$n(\mathfrak{D}_{ik}) \geqq n(\mathfrak{J}_i \times \mathfrak{D}_{ik});$$

nach (42) ergibt sich also

$$n(\mathfrak{J}_i \times \mathfrak{D}_{ik}) \leqq n(\mathfrak{d}_{ik}),$$

woraus zusammen mit $\mathfrak{J}_i \times \mathfrak{D}_{ik} < \mathfrak{d}_{ik}$ die erste Gleichung (41) folgt; die zweite ergibt sich analog.

Eine weitere wichtige Beziehung erhält man aus der Gleichung

$$\mathfrak{d}_{ik} = \bar{\mathfrak{d}}_{ki}.$$

Wendet man auf sie (41) an, so erhält man

$$\mathfrak{J}_i \times \mathfrak{D}_{ik} = \overline{\mathfrak{D}_{ki} \times \mathfrak{J}_i} = \mathfrak{J}_i \times \bar{\mathfrak{D}}_{ki}.$$

Bildet man beiderseits den Durchschnitt mit $\mathfrak{O}$, so erhält man links $\mathfrak{D}_{ik}$, rechts ein $\bar{\mathfrak{D}}_{ik}$ umfassendes Ideal:

$$\mathfrak{D}_{ik} > \bar{\mathfrak{D}}_{ki}.$$

Es ist aber $n(\mathfrak{d}_{ik}) = n(\mathfrak{d}_{ki})$, nach (42) also $n(\mathfrak{D}_{ik}) = n(\mathfrak{D}_{ki})$, somit

$$\mathfrak{D}_{ik} = \bar{\mathfrak{D}}_{ki}. \tag{43}$$

Die soeben in einem Spezialfalle bewiesene Tatsache, *daß* $\mathfrak{D}_{ik} = \mathfrak{A}$ *ist, sobald* $\mathfrak{A} < \mathfrak{O} < \mathfrak{J}_i \cap \mathfrak{J}_k$ *und* $\mathfrak{J}_i \times \mathfrak{A} = \mathfrak{d}_{ik}$ *gilt, ist allgemein richtig.* Denn es ist offensichtlich $\mathfrak{D}_{ik} > \mathfrak{A}$. Andererseits ist $\mathfrak{A}\,\bar{\mathfrak{A}}\,\frac{1}{n(\mathfrak{A})} = \mathfrak{O}$ und nach § 2 $\mathfrak{J}_i = \mathfrak{d}_{ik}\bar{\mathfrak{d}}_{ik}\frac{1}{n(\mathfrak{d}_{ik})}$, also

$$\mathfrak{d}_{ik}\bar{\mathfrak{d}}_{ik}\frac{1}{n(\mathfrak{A})} = (\mathfrak{J}_i \times \mathfrak{A})\,\overline{(\mathfrak{J}_i \times \mathfrak{A})}\,\frac{1}{n(\mathfrak{A})} = \mathfrak{J}_i \times \mathfrak{O} \times \mathfrak{J}_i = \mathfrak{J}_i = \mathfrak{d}_{ik}\bar{\mathfrak{d}}_{ik}\frac{1}{n(\mathfrak{d}_{ik})},$$

woraus sich $n(\mathfrak{A}) = n(\mathfrak{d}_{ik})$ ergibt, und dies hat zusammen mit (42) und $\mathfrak{D}_{ik} > \mathfrak{A}$ die Gleichung

$$\mathfrak{D}_{ik} = \mathfrak{A}$$

zur Folge.

6. Nach diesen Vorbereitungen kann nun der Beweis des ersten Teiles von Satz 13 bzw. der ihm äquivalenten, in **5** ausgesprochenen Aussage in Angriff genommen werden. Der erste Schritt besteht in einer Abbildung von Distanzidealen auf Ideale

---

[23]) Vl. Kořínek, Kvadraticka tělesa v kvaternionových okruzích. Věstník, Král. Čes., Spol. Nauk, Tř. II, 1930, S. 1. Ähnliche Betrachtungen findet man auch bei Hasse, Über gewisse Ideale in einer einfachen Algebra, Actualités Scientifiques et Industrielles **109** (1934); Exposés mathématiques publiés à la mémoire de Jaques Herbrand, I.

in $\mathfrak{O}$. Das Ideal $\mathfrak{d}_{12} + \mathfrak{d}_{32}$ teilt die Distanzideale $\mathfrak{d}_{12}$ und $\mathfrak{d}_{32}$ von rechts, und ist daher selbst ein Distanzideal [22]) zwischen einer neuen Maximalordnung $\mathfrak{J}_6$ und $\mathfrak{J}_2$:

$$\mathfrak{d}_{12} + \mathfrak{d}_{32} = \mathfrak{d}_{62}\,. \tag{44}$$

(Der Fall $\mathfrak{J}_2 = \mathfrak{J}_6$ ist keineswegs ausgeschlossen; er führt, was nur nebenbei bemerkt sei, auf die Gleichung $\mathfrak{J}_1 \cap \mathfrak{J}_2 \cap \mathfrak{J}_3 = \mathfrak{J}_1 \cap \mathfrak{J}_3$.) Nach (41) ist

$$\mathfrak{O} \cap \mathfrak{d}_{62} = \mathfrak{O} \cap (\mathfrak{D}_{12} \times \mathfrak{J}_2 + \mathfrak{D}_{32} \times \mathfrak{J}_2) = \mathfrak{O} \cap ((\mathfrak{D}_{12} + \mathfrak{D}_{32}) \times \mathfrak{J}_2)\,.$$

Die Linksordnung $\mathfrak{J}_6$ des Ideals $\mathfrak{d}_{12} + \mathfrak{d}_{32} = (\mathfrak{D}_{12} + \mathfrak{D}_{32}) \times \mathfrak{J}_2$ enthält $\mathfrak{O}$, denn $(\mathfrak{D}_{12} + \mathfrak{D}_{32}) \times \mathfrak{J}_2$ gestattet linksseitige Multiplikation mit $\mathfrak{O}$. Nun ist nach dem am Schluß von 5 erwähnten Hilfssatze

$$\mathfrak{D}_{62} = \mathfrak{O} \cap \mathfrak{d}_{62} = \mathfrak{D}_{12} + \mathfrak{D}_{32}\,. \tag{45}$$

$\mathfrak{D}_{62}$ teilt die Ideale $\mathfrak{D}_{12}$ und $\mathfrak{D}_{32}$, d. h. es gibt ganze Ideale $\mathfrak{D}'_{16}$, $\mathfrak{D}'_{36}$ derart, daß

$$\mathfrak{D}_{12} = \mathfrak{D}'_{16} \cdot \mathfrak{D}_{62}\,, \qquad \mathfrak{D}_{32} = \mathfrak{D}'_{36} \cdot \mathfrak{D}_{62} \tag{46}$$

ist. Multipliziert man diese Gleichungen links mit $\mathfrak{J}_1$ bzw. $\mathfrak{J}_3$ und rechts mit $\mathfrak{J}_2$, so erhält man

$$\mathfrak{J}_1 \times \mathfrak{D}_{12} \times \mathfrak{J}_2 = \mathfrak{d}_{12} = (\mathfrak{J}_1 \times \mathfrak{D}'_{16}) \times \mathfrak{d}_{62}\,,$$
$$\mathfrak{J}_3 \times \mathfrak{D}_{32} \times \mathfrak{J}_2 = \mathfrak{d}_{32} = (\mathfrak{J}_3 \times \mathfrak{D}'_{36}) \times \mathfrak{d}_{62}\,,$$

und beachtet man, daß $\mathfrak{d}_{62}$ wegen (44) von rechts in $\mathfrak{d}_{12}$ und $\mathfrak{d}_{32}$ aufgeht, so wird jetzt

$$\mathfrak{d}_{12}\mathfrak{d}_{62}^{-1} = \mathfrak{d}_{16} = \mathfrak{J}_1 \times \mathfrak{D}'_{16} \times \mathfrak{J}_6\,,$$
$$\mathfrak{d}_{32}\mathfrak{d}_{62}^{-1} = \mathfrak{d}_{36} = \mathfrak{J}_3 \times \mathfrak{D}'_{36} \times \mathfrak{J}_6\,.$$

Aus diesen Gleichungen erhält man

$$\mathfrak{D}'_{16} < \mathfrak{D}_{16}, \qquad \mathfrak{D}'_{36} < \mathfrak{D}_{36}\,.$$

Andererseits ist aber nach (46)

$$n(\mathfrak{D}'_{16}) = \frac{n(\mathfrak{D}_{12})}{n(\mathfrak{D}_{62})}, \qquad n(\mathfrak{D}'_{36}) = \frac{n(\mathfrak{D}_{32})}{n(\mathfrak{D}_{62})}$$

und nach (42)

$$n(\mathfrak{D}_{16}) = n(\mathfrak{d}_{16}) = \frac{n(\mathfrak{d}_{12})}{n(\mathfrak{d}_{62})}, \qquad n(\mathfrak{D}_{36}) = n(\mathfrak{d}_{36}) = \frac{n(\mathfrak{d}_{32})}{n(\mathfrak{d}_{62})}\,,$$

also

$$n(\mathfrak{D}_{16}) = n(\mathfrak{D}'_{16}), \qquad n(\mathfrak{D}_{36}) = n(\mathfrak{D}'_{36})\,,$$

woraus sich $\mathfrak{D}_{16} = \mathfrak{D}'_{16}$, $\mathfrak{D}_{36} = \mathfrak{D}'_{36}$ ergibt, also

$$\mathfrak{D}_{12} = \mathfrak{D}_{16}\mathfrak{D}_{62}, \qquad \mathfrak{D}_{32} = \mathfrak{D}_{36}\mathfrak{D}_{62}\,. \tag{47}$$

Diese Gleichungen sind ein Bild der Eigenschaften der Distanzideale in Idealen von $\mathfrak{O}$; wir brauchen noch eine dritte:

$$\mathfrak{D}_{31} = \mathfrak{D}_{36}\,\mathfrak{D}_{61}\,. \tag{48}$$

Beweis. Es ist

$$\mathfrak{d}_{16} + \mathfrak{d}_{36} = \mathfrak{d}_{12}\mathfrak{d}_{62}^{-1} + \mathfrak{d}_{32}\mathfrak{d}_{62}^{-1} = (\mathfrak{d}_{12} + \mathfrak{d}_{32})\mathfrak{d}_{62}^{-1}\,,$$

und nach (44)

$$\mathfrak{d}_{16} + \mathfrak{d}_{36} = \mathfrak{J}_6\,.$$

Daraus erhält man

$$\mathfrak{d}_{16}\mathfrak{d}_{63} + \mathfrak{d}_{36}\mathfrak{d}_{63} = \mathfrak{d}_{16}\mathfrak{d}_{63} + \mathfrak{J}_3\, n(\mathfrak{d}_{36}) = \mathfrak{d}_{63}\,. \tag{49}$$

$\mathfrak{d}_{16}\mathfrak{d}_{63}$ ist ein ganzes Ideal der Linksordnung $\mathfrak{J}_1$ und der Rechtsordnung $\mathfrak{J}_3$, es gibt

daher ein ganzes Ideal $\mathfrak{a}$ der Links- und Rechtsordnung $\mathfrak{J}_3$ so, daß

$$\mathfrak{d}_{16}\mathfrak{d}_{63} = \mathfrak{d}_{13}\mathfrak{a}$$

ist. $\mathfrak{a}$ hat entweder die Gestalt $\mathfrak{a} = \mathfrak{J}_3 a$, wobei a ganz und rational ist, oder $n(\mathfrak{a})$ hat mit der Diskriminante der Algebra einen gemeinsamen Primteiler. Dieser müßte nach dem Normenmultiplikationssatze in $n(\mathfrak{d}_{16})$ oder $n(\mathfrak{d}_{63})$ aufgehen, was aber der Eigenschaft eines Distanzideals widerspricht [22]). Letzterer Fall kommt also nicht in Frage. Ein von ± 1 verschiedener gemeinsamer Teiler von a und $n(\mathfrak{d}_{36})$ geht nach (49) in $\mathfrak{d}_{63}$ auf; das widerspricht ebenfalls der Eigenschaft eines Distanzideals [22]). Ist aber $a \neq \pm 1$ und zu $n(\mathfrak{d}_{36})$ teilerfremd, so teilt a das Distanzideal

$$\mathfrak{d}_{16} = \mathfrak{d}_{13}\mathfrak{d}_{63}^{-1} a;$$

auch das ist ein Widerspruch. Somit ist $a = \pm 1$ und

$$\mathfrak{d}_{16}\mathfrak{d}_{63} = \mathfrak{d}_{13}.$$

Nach (41) ergibt diese Gleichung

$$\mathfrak{J}_1 \times \mathfrak{D}_{16} \times \mathfrak{J}_6 \times \mathfrak{D}_{63} = \mathfrak{J}_1 \times \mathfrak{D}_{16} \cdot \mathfrak{D}_{63} = \mathfrak{J}_1 \times \mathfrak{D}_{13},$$

woraus (48) nach dem am Schluß von **5** erwähnten Hilfssatze und (43) folgt.

Der zweite Schritt des Beweises besteht in der Zerlegung der Ideale $\mathfrak{D}_{6i}$ $(i = 1,2,3)$ in Produkte

$$\mathfrak{D}_{6i} = \mathfrak{A}_{6i}\mathfrak{B}_{6i} \tag{50}$$

ganzer Ideale derart, daß $\mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}\overline{\mathfrak{B}}_{61}\overline{\mathfrak{B}}_{62}\overline{\mathfrak{B}}_{63}$ ein primitives Ideal wird. Die Ideale $\mathfrak{D}_{6i}$ sind selbst primitiv, da sonst wegen (41) auch die Distanzideale $\mathfrak{d}_{6i}$ nicht primitiv sein würden. Sie haben zu je zweien keinen ambigen Primteiler gemeinsam; denn wäre $\mathfrak{P}$ ein solcher, so müßte wegen (47) und (48) $\mathfrak{P}^2$ in $\mathfrak{D}_{12}$, $\mathfrak{D}_{32}$ oder $\mathfrak{D}_{13}$ aufgehen, und dann wäre eins der Distanzideale $\mathfrak{d}_{12}$, $\mathfrak{d}_{32}$, $\mathfrak{d}_{13}$ nicht primitiv. Das wäre ein Widerspruch.

Wir zerlegen die $\mathfrak{D}_{6i}$ in Primzahlpotenzen:

$$\mathfrak{D}_{6i} = \mathfrak{P}_{i1}^{a_{i1}} \cdot \mathfrak{P}_{i2}^{a_{i2}} \cdots \mathfrak{P}_{in_i}^{a_{in_i}}. \tag{51}$$

Nun setzen wir $\mathfrak{A}_{61} = \mathfrak{D}_{61}$, $\mathfrak{B}_{61} = \mathfrak{O}$. In $\mathfrak{A}_{62}$ nehmen wir die Faktoren $\mathfrak{P}_{2r}^{a_{2r}}$ auf, für welche $(\overline{\mathfrak{P}}_{2r}, \mathfrak{D}_{61}) = \mathfrak{O}$ ist, in $\mathfrak{B}_{62}$ dagegen die $\mathfrak{P}_{2r}^{a_{2r}}$, für welche $(\overline{\mathfrak{P}}_{2r}, \mathfrak{D}_{61}) = \overline{\mathfrak{P}}_{2r}$ ist. Da $\mathfrak{D}_{61}$ und $\mathfrak{D}_{62}$ keinen gemeinsamen ambigen Primteiler besitzen, ist jetzt $\mathfrak{A}_{61}\mathfrak{A}_{62}\overline{\mathfrak{B}}_{61}\overline{\mathfrak{B}}_{62}$ primitiv. Entsprechend kann mit $\mathfrak{D}_{63}$ verfahren werden.

Ist jetzt $\mathfrak{J}_4$ die Rechtsordnung von $\mathfrak{J}_6 \times \mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}$ und $\mathfrak{J}_5$ die von $\mathfrak{J}_6 \times \mathfrak{B}_{61}\mathfrak{B}_{62}\mathfrak{B}_{63}$, so behaupte ich

$$\mathfrak{J}_1 \cap \mathfrak{J}_2 \cap \mathfrak{J}_3 = \mathfrak{J}_4 \cap \mathfrak{J}_5.$$

Im dritten Schritt des Beweises zeigen wir, daß $\mathfrak{J}_6 \times \mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}$, $\mathfrak{J}_6 \times \mathfrak{B}_{61}\mathfrak{B}_{62}\mathfrak{B}_{63}$ und $\mathfrak{J}_5 \times \mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}\overline{\mathfrak{B}}_{61}\overline{\mathfrak{B}}_{62}\overline{\mathfrak{B}}_{63}$ Distanzideale sind. $\mathfrak{J}_6 \times \mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}$ und $\mathfrak{J}_6 \times \mathfrak{B}_{61}\mathfrak{B}_{62}\mathfrak{B}_{63}$ gestatten rechtsseitige Multiplikation mit $\mathfrak{O}$, also ist $\mathfrak{O} < \mathfrak{J}_4$ und $\mathfrak{O} < \mathfrak{J}_5$. Die Ideale $\mathfrak{J}_6 \times \mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}$, $\mathfrak{J}_6 \times \mathfrak{B}_{61}\mathfrak{B}_{62}\mathfrak{B}_{63}$ und $\mathfrak{J}_5 \times \mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}\overline{\mathfrak{B}}_{61}\overline{\mathfrak{B}}_{62}\overline{\mathfrak{B}}_{63}$ sind ganz; ferner sind sie primitiv, da $\mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}$, $\overline{\mathfrak{B}}_{61}\overline{\mathfrak{B}}_{62}\overline{\mathfrak{B}}_{63}$ und $\mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}\overline{\mathfrak{B}}_{61}\overline{\mathfrak{B}}_{62}\overline{\mathfrak{B}}_{63}$ primitiv sind. Ihre Normen teilen die Normen von $\mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}$, $\mathfrak{B}_{61}\mathfrak{B}_{62}\mathfrak{B}_{63}$ und $\mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}\overline{\mathfrak{B}}_{61}\overline{\mathfrak{B}}_{62}\overline{\mathfrak{B}}_{63}$, sie haben daher mit der Diskriminante der Algebra keinen Primteiler gemeinsam; ein solcher würde nämlich wegen (50) und (42) in $n(\mathfrak{d}_{61})$, $n(\mathfrak{d}_{62})$ oder $n(\mathfrak{d}_{63})$ aufgehen, was aber der Eigenschaft eines Distanzideals widerspricht [22]). Somit sind diese Ideale selbst Distanzideale [22]), insbesondere also

$$\mathfrak{J}_6 \times \mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63} = \mathfrak{d}_{64}, \qquad \mathfrak{J}_6 \times \mathfrak{B}_{61}\mathfrak{B}_{62}\mathfrak{B}_{63} = \mathfrak{d}_{65}.$$

Aus dem am Schluß von 5 erwähnten Hilfssatze erhält man jetzt

$$\mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63} = \mathfrak{D}_{64}, \quad \mathfrak{B}_{61}\mathfrak{B}_{62}\mathfrak{B}_{63} = \mathfrak{D}_{65}.$$

Nach (43) wird ferner

$$\overline{\mathfrak{B}}_{61}\overline{\mathfrak{B}}_{62}\overline{\mathfrak{B}}_{63} = \mathfrak{D}_{56}$$

und nach (41), wenn man beachtet, daß auch $\mathfrak{J}_5 \times \mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}\overline{\mathfrak{B}}_{61}\overline{\mathfrak{B}}_{62}\overline{\mathfrak{B}}_{63}$ ein Distanzideal ist,

$$(52)\quad \mathfrak{J}_5 \times \mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}\overline{\mathfrak{B}}_{61}\overline{\mathfrak{B}}_{62}\overline{\mathfrak{B}}_{63} = \mathfrak{d}_{56}(\mathfrak{J}_6 \times \mathfrak{A}_{61}\mathfrak{A}_{62}\mathfrak{A}_{63}) = \mathfrak{d}_{56}\mathfrak{d}_{64} = \mathfrak{d}_{54}.$$

Der vierte Schritt liefert nun schnell das Schlußergebnis. $\mathfrak{d}_{62}$ teilt nach (44) das Ideal $\mathfrak{d}_{12}$ von rechts, nach Satz 14 enthält $\mathfrak{J}_6$ daher den Durchschnitt $\mathfrak{J}_1 \cap \mathfrak{J}_2$. Daraus folgt

$$\mathfrak{J}_1 \cap \mathfrak{J}_2 \cap \mathfrak{J}_3 = (\mathfrak{J}_1 \cap \mathfrak{J}_6) \cap (\mathfrak{J}_2 \cap \mathfrak{J}_6) \cap (\mathfrak{J}_3 \cap \mathfrak{J}_6)$$

und nun nach (39)

$$(53)\quad \mathfrak{J}_1 \cap \mathfrak{J}_2 \cap \mathfrak{J}_3 = [1, \mathfrak{J}_6 \times \mathfrak{D}_{61}] \cap [1, \mathfrak{J}_6 \times \mathfrak{D}_{62}] \cap [\mathfrak{J}_6 \times \mathfrak{D}_{63}].$$

Es mögen jetzt die rationalen Primzahlen, in denen die $\mathfrak{P}_{ir}$ aufgehen, mit p_{ir} bezeichnet werden; sie sind für ein festes i voneinander verschieden, denn würden etwa $\mathfrak{P}_{i1}$ und $\mathfrak{P}_{i2}$ in derselben rationalen Primzahl aufgehen, so müßte $\mathfrak{P}_{i1} = \overline{\mathfrak{P}}_{i2}$ sein, $\mathfrak{D}_{6i}$ wäre also nicht primitiv. Ist $p_{ir}^{k_{ir}}$ die größte $|\mathfrak{J}_6 \cap \mathfrak{J}_i|$ teilende Potenz von p_{ir} (nebenbei bemerkt ist $k_{ir} = a_{ir}$), so wird

$$\mathfrak{J}_6 \cap \mathfrak{J}_i = ([1, \mathfrak{J}_6 \times \mathfrak{D}_{6i}] + \mathfrak{J}_6 p_{i1}^{k_{i1}}) \cap ([1, \mathfrak{J}_6 \times \mathfrak{D}_{6i}] + \mathfrak{J}_6 p_{i2}^{k_{i2}}) \cap \cdots \cap ([1, \mathfrak{J}_6 \times \mathfrak{D}_{6i}] + \mathfrak{J}_6 p_{ini}^{k_{ini}})$$
$$= [1, \mathfrak{J}_6 \times \mathfrak{P}_{i1}^{a_{i1}}] \cap [1, \mathfrak{J}_6 \times \mathfrak{P}_{i2}^{a_{i2}}] \cap \cdots \cap [1, \mathfrak{J}_6 \times \mathfrak{P}_{ini}^{a_{ini}}]\ ^{24})$$

und

$$(54)\quad \mathfrak{J}_1 \cap \mathfrak{J}_2 \cap \mathfrak{J}_3 = [1, \mathfrak{J}_6 \times \mathfrak{P}_{11}^{a_{11}}] \cap \cdots \cap [1, \mathfrak{J}_6 \times \mathfrak{P}_{3n_3}^{a_{3n_3}}].$$

Analog wird mit $\mathfrak{J}_4 \cap \mathfrak{J}_5$ verfahren. Nach (52) und Satz 14 ist $\mathfrak{J}_6 > \mathfrak{J}_4 \cap \mathfrak{J}_5$, also wird

$$\mathfrak{J}_4 \cap \mathfrak{J}_5 = (\mathfrak{J}_4 \cap \mathfrak{J}_6) \cap (\mathfrak{J}_5 \cap \mathfrak{J}_6),$$

und wenn (51) auch als Primidealzerlegung von $\mathfrak{D}_{64}$ und $\mathfrak{D}_{65}$ angesehen wird, gilt entsprechend (54) die Gleichung

$$(55)\quad \mathfrak{J}_4 \cap \mathfrak{J}_5 = [1, \mathfrak{J}_6 \times \mathfrak{P}_{41}^{a_{41}}] \cap \cdots \cap [1, \mathfrak{J}_6 \times \mathfrak{P}_{5n_5}^{a_{5n_5}}].$$

Nun sind wegen (50) und der Konstruktion der $\mathfrak{A}_{6i}$, $\mathfrak{B}_{6i}$ die in (54) und (55) auftretenden $\mathfrak{P}_{ir}^{a_{ir}}$ bis auf die Reihenfolge identisch, und daher ist in der Tat

$$\mathfrak{J}_1 \cap \mathfrak{J}_2 \cap \mathfrak{J}_3 = \mathfrak{J}_4 \cap \mathfrak{J}_5.$$

7. Zum Schluß kommen wir auf das Problem zurück, die Anzahl der Maximalordnungen zu bestimmen, die eine gegebene primitive Ordnung enthalten. Eine explizite Formel läßt sich nur in folgendem Spezialfalle angeben:

Satz 16 [25]**.** *Es sei* $\mathfrak{o}$ *eine primitive Ordnung und*

$$|\mathfrak{o}| = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$$

---

[24]) Diese Behauptung besagt soviel wie die andere, daß die $\mathfrak{J}_6 \cap \mathfrak{J}_i$ die Durchschnitte ihrer p-adischen Grenzmengen für sämtliche p sind. Vgl. H. Hasse, Über $\wp$-adische Schiefkörper und ihre Bedeutung für die Arithmetik der hyperkomplexen Zahlsysteme, Math. Annalen **104** (1931), S. 495.

[25]) Die Übereinstimmung des Satzes 16 mit dem Fueterschen Ergebnis [5]) ist nicht auf den ersten Blick zu erkennen. Es sei $\mathfrak{o} = [1, \omega, \Omega, \omega\Omega]$ eine Ordnung, die den Bedingungen des ersten Fueterschen Hauptsatzes

die Zerlegung der Determinante in Primzahlpotenzen. Für $1 \leqq r \leqq n_1$ *sei* $(\mathfrak{o}/p_r) = 1$ *und für* $n_1 < r \leqq n$ $(\mathfrak{o}/p_r) = -1$. *Dann ist* $\mathfrak{o}$ *in* $(a_1 + 1)(a_2 + 1) \cdots (a_{n_1} + 1)$ *Maximalordnungen enthalten.*

Beweis. Ist $n_1 = n$, so ist nach Satz 13 $\mathfrak{o}$ Durchschnitt von zwei Maximalordnungen; jetzt kommt Satz 15 zur Anwendung und liefert die behauptete Anzahlformel.

Satz 16 sei für $n - n_1 = n_2$ schon bewiesen, und nun sei $n - n_1 = n_2 + 1 > 1$. Nach 1 ist die Erweiterungsordnung $\mathfrak{o}_1$ von $\mathfrak{o}$ zu p_n in ebenso vielen Maximalordnungen wie $\mathfrak{o}$ enthalten. Nach Satz 12 ist

$$|\mathfrak{o}_1| = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_{n-2}}$$

die Zerlegung von $|\mathfrak{o}_1|$ in Primzahlpotenzen; die Richtigkeit des Satzes 16 folgt nun aus der Induktionsvoraussetzung.

---

genügt. Die Zahl f dort ist gleich der Determinante $|\mathfrak{o}|$ in unserer Bezeichnung. Die Bedingung, daß $\frac{\omega - \overline{\omega}}{n}$ bzw. $\frac{\omega - \overline{\omega}}{2n}$ für jede natürliche Zahl n nicht zugleich ganz und mit Ω konkordant sein soll, hat die Primitivität von $\mathfrak{o}$ zur Folge.

Es muß nun, um Satz 16 anwenden zu können, $(\mathfrak{o}/p) \neq 0$ angenommen werden. Die Anzahl der $\mathfrak{o}$ enthaltenden Maximalordnungen wird hier, wie bei Fueter, durch ein Produkt gegeben, dessen Faktoren die einzelnen Primzahlpotenzteiler von $|\mathfrak{o}| = f$ sind; es genügt daher, diese zu vergleichen.

Ist p eine f teilende Primzahl, und ist $(\Delta(\omega)/p) = -1$, so zerfällt p in $k(\omega)$ nicht, liefert also den Beitrag 1. Andererseits ist nach Satz 10 jetzt $(\mathfrak{o}/p) = -1$, und auch nach Satz 16 liefert p den Beitrag 1.

Ist $(\Delta(\omega)/p) = 1$, so zerfällt p in $k(\omega)$; geht p a-mal in f auf, so liefert p^a nach Fueter den Beitrag $a + 1$. Denselben liefert p^a nach Satz 16, da nach Satz 10 $(\mathfrak{o}/p) = 1$ ist.

Ist schließlich $(\Delta(\omega)/p) = 0$, so lehrt eine eingehendere Diskussion, daß unter den gemachten Voraussetzungen nur $(\mathfrak{o}/p) = 1$ sein kann, und daß p nur einmal in f aufgeht. Jetzt liefert p sowohl nach dem I. Fueterschen Hauptsatz wie nach Satz 16 den Beitrag 2.

Eingegangen 8. Juni 1935.

Über Klassenzahlrelationen quadratischer Formen in quadratischen Körpern.

Von *S. Lubelski* in Warschau.

Herglotz [1]) hat eine Formel aufgestellt, mittels welcher man die Klassenzahl H eines algebraischen Körpers K berechnen kann, der durch Zusammensetzung von m quadratischen Körpern K_g $(g = 1, 2, \ldots, m)$ entsteht. Aus dieser Formel ergibt sich unmittelbar, daß die Klassenzahl des Körpers K durch das Produkt der Klassenzahlen $h_1 h_2 \cdots h_m$ teilbar ist, wo h_g die Klassenzahl des Körpers K_g bedeutet. Wenn $m = 2$ ist, kann K als relativ-quadratischer Körper angesehen werden. Dann kann man leicht den Zusammenhang zwischen den Idealklassen des biquadratischen Körpers resp. des relativ-quadratischen Körpers mit binären quadratischen Formen, deren Koeffizienten Idealzahlen des Grundkörpers k sind, darstellen, wobei die Determinanten der Formen der relativen Diskriminante von K gleich sind.

Wollen wir aber nur mit binären quadratischen Formen operieren, deren Koeffizienten ganze algebraische Zahlen sind, dann ist die Sachlage anders. Das Ziel dieser Arbeit ist nämlich der Beweis für den folgenden

Satz. *Es sei* $K(\sqrt{-q})$, $q \neq 2$ *Primzahl, ein imaginär-quadratischer Körper mit ungerader Klassenzahl,* $D > 2$ *eine natürliche Zahl, die für* $q = 1$ *größer als* 12 *ist und für welche* $D' = \frac{D}{4}$ *eine ganze durch keine Quadratzahl des Körpers* $K(\sqrt{-q})$ *teilbare Zahl ist; ferner sei* h *die Klassenzahl der binären quadratischen Formen der Determinante* D, h' *die Klassenzahl der binären quadratischen Formen der Determinante* $-qD$ *im Körper der rationalen Zahlen. Dann gilt:*

Die Klassenzahl H *der binären quadratischen Formen der Determinante* D, *deren Koeffizienten ganze Zahlen des Körpers* $K(\sqrt{-q})$ *sind, ist* $H = \frac{hh'}{2}$ *für* $q \geqq 3$. *Ist* $q = 1$, *so ist* $H = hh'$ *oder* $2hh'$, *je nachdem* $x^2 - D'y^2 = -1$ *in ganzen rationalen Zahlen lösbar ist oder nicht.*

Die folgenden Werke werden in dieser Arbeit oft benutzt:

1. E. Cahen, Theorie des Nombres II, Paris 1924. Zitiert mit Cahen,
2. D. Hilbert, Über die Theorie des relativ quadratischen Zahlkörpers, Werke I, S. 370 bis 482. Zitiert mit Hilbert.

Erster Teil.

Vorbemerkung. Die ganzen Idealzahlen im Sinne von Kronecker-Weber, sogenannte ganze Funktionale [2]), oder die ganzen endlichen Idealzahlen im Sinne von H. Prüfer [3])

[1]) G. Herglotz, Über einen Dirichletschen Satz, Math. Zeitschr. **12** (1922), S. 255—261.

[2]) H. Weber, Lehrbuch der Algebra **2** (Braunschweig 1896), S. 489—557.

[3]) H. Prüfer, Neue Begründung der algebraischen Zahlentheorie, Math. Annalen **94** (1925), S. 198—243.

bilden einen Integritätsbereich, in welchem jede ganze Idealzahl eindeutig (sofern assoziierte Idealzahlen als nicht verschieden angesehen werden) als Produkt von endlich vielen Primidealzahlen darstellbar ist.

Bezeichnung 1. Mit k werden wir stets den zugrunde gelegten endlichen algebraischen Zahlkörper, mit G den Integritätsbereich bezeichnen, welcher die ganzen algebraischen Zahlen des Grundkörpers k enthält. Mit $\bar{G}$ bezeichnen wir den Integritätsbereich, der die ganzen Idealzahlen des Körpers k enthält.

Bezeichnung 2. Mit D wollen wir die Determinante der Form $ax^2 + bxy + cy^2$ bezeichnen, deren Koeffizienten zu $\bar{G}$ gehören.

Definition 1. Zwei binäre quadratische Formen $ax^2 + bxy + cy^2$, $a_1x^2 + b_1xy + c_1y^2$ mit Koeffizienten aus dem Integritätsbereich $\bar{G}$ bezeichnen wir als eigentlich äquivalent, wenn mittels einer Transformation $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $\alpha\delta - \beta\gamma = 1$, wo $\alpha, \beta, \gamma, \delta$ ebenfalls zu $\bar{G}$ gehören, die eine Form in die andere übergeht. Ist $\alpha\delta - \beta\gamma = -1$, so nennen wir die Formen uneigentlich äquivalent.

Wie im rationalen Körper gehen wir von der grundlegenden Lagrangeschen Identität aus:

$$(ax^2 + bxy + a'cy^2)\,(a'x'^2 + bx'y' + acy'^2) = aa'X^2 + bXY + cY^2\,,$$
$$X = xx' - cyy', \quad Y = axy' + a'x'y' + byy'.$$

Definition 2. Zwei Formen nennen wir komponierbar, wenn die eine von der Gestalt $ax^2 + bxy + a'cy^2$ und die andere von der Gestalt $a'x^2 + bxy + acy^2$ ist.

Wie im rationalen Integritätsbereich können wir auch für $\bar{G}$ den folgenden Satz beweisen:

Hilfssatz 1. *Das Produkt zweier komponierbarer Formen, von denen eine die Zahl m, die andere die Zahl m' eigentlich darstellt, stellt die Zahl mm' eigentlich dar* (vgl. Cahen S. 471).

Hilfssatz 2. *Jede binäre quadratische Form $f(x, y) = ax^2 + bxy + cy^2$ mit Koeffizienten aus $\bar{G}$ stellt Idealzahlen dar, welche relativ prim sind zu einer beliebigen Idealzahl m; dabei kann man x, y als ganze algebraische Zahlen annehmen.*

Beweis. Es sei zunächst m eine Primidealzahl. Ist a resp. c durch m nicht teilbar, so kann man entweder $x = 1, y = 0$ oder $x = 0, y = 1$ setzen. Sind a und c durch m teilbar, so muß, da $f(x, y)$ primitiv ist, $(b, m) = 1$ sein, und demnach ist $f(1, 1)$ die entsprechende Zahl. Es seien jetzt $m_1, m_2, \ldots, m_u$ die verschiedenen Primidealteiler von m. Bezeichnen wir mit x_n, y_n die Zahlen, für welche $(f(x_n, y_n), m_n) = 1$ ist, so findet man im Integritätsbereich G Zahlen x, y, für welche gleichzeitig

$$x \equiv x_n \pmod{m_n}, \quad y \equiv y_n \pmod{m_n} \qquad (n = 1, 2, \ldots, u)$$

ist. Es gilt nämlich z. B. für $u = 2$, daß eine Zahl w_1 existiert, für die $m_1 | w_1$ und $(m_2, w_1) = 1$ ist. Desgleichen existiert eine Zahl w_2, für die $(w_1, w_2) = 1$ und $m_2 | w_2$ ist. Die unbestimmte Gleichung $x_2 - x_1 = w_1t - w_2t$ ist in Zahlen des Integritätsbereiches G lösbar. Durch Induktion können wir den Satz für beliebiges u beweisen. Somit erhalten wir auch den folgenden Satz:

Hilfssatz 3. *Zu zwei beliebigen binären quadratischen Formen gibt es immer zwei andere, die diesen Formen äquivalent und die miteinander komponierbar sind* (vgl. Cahen S. 473).

Teilen wir alle binären quadratischen Formen einer Determinante D in Klassen ein durch die Festsetzung, daß zwei Formen zur selben Klasse gehören, wenn sie nur eigentlich äquivalent sind, so bilden diese Klassen, dem Hilfssatze 3 gemäß, eine abelsche Gruppe. Es ist evident, daß auch hier $ax^2 + bxy + cy^2$ und $ax^2 - bxy + cy^2$ als inverse Formen und $x^2 - Dy^2$ resp. $x^2 + xy - \frac{D-1}{4}y^2$ als Hauptformen erscheinen.

Endlich kann man, wie im rationalen Integritätsbereich, den folgenden Satz beweisen:

Hilfssatz 4. *Es sei* $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, *wo* $p_1, p_2, \dots, p_n$ *Primidealteiler sind und* p_g $(g = 1, 2, \dots, n)$ *durch die Formen* C_g *und* C_g^{-1} *darstellbar ist. Dann ist* m *eigentlich durch das Produkt der Formen* $C_1^{\pm\alpha_1} C_2^{\pm\alpha_2} \dots C_n^{\pm\alpha_n}$ *und nur durch dieses Produkt darstellbar.*

Beweis. Die Kongruenz

$$x^2 + \varrho x - d \equiv 0 \pmod{p_g^{\alpha_g}}, \quad \varrho = 0, d = D; \ \varrho = 1, d = \frac{D-1}{4}$$

hat höchstens zwei Lösungen. Ist eine Lösung l, so ist die zweite $-\varrho - l$. Die Idealzahl $p_g^{\alpha_g}$ ist also durch die Formen

$$p_g^{\alpha_g} x^2 \pm (2l + \varrho)\, xy + \frac{l^2 + \varrho l - d}{p_g^{\alpha_g}} y^2$$

eigentlich darstellbar. Dabei sind dies die einzigen Formen, durch welche $p_g^{\alpha_g}$ eigentlich darstellbar sein kann. Man hat nämlich symbolisch für entsprechende b und c, daß

$$(p^\alpha x^2 + bxy + cy^2) = (px^2 + bxy + p^{\alpha-1} cy^2)^\alpha$$

(vgl. z. B. Cahen S. 478), und ferner gilt symbolisch die Produktrelation

$$(ax^2 + bxy + cy^2) = \left(p_1^{\alpha_1} x^2 + bxy + c\frac{m}{p_1^{\alpha_1}} y^2\right)\left(p_2^{\alpha_2} x^2 + bxy + c\frac{m}{p_2^{\alpha_2}} y^2\right)\cdots.$$

Hilfssatz 5. *Ist* $\mathfrak{d}$ *die Relativdiskriminante des relativ-quadratischen Körpers* $K(\sqrt{D})$ *mit* $k(\sqrt{-q})$ *als Grundkörper, in welchem* $\frac{D}{4} = D'$ *quadratfrei ist, so ist für ganzrationales* D'

1. $\mathfrak{d} = D'$ *für* $q = 1$ *stets und für* $q \equiv 3 \pmod 4$, *wenn* $D' \equiv 1 \pmod 4$,
2. $\mathfrak{d} = D$ *für* $q \equiv 3 \pmod 4$, *wenn* $D' \equiv -1, 2 \pmod 4$ *ist.*

Beweis. Der Definition der Relativdiskriminante gemäß haben wir:

$$\mathfrak{d} = (\Omega_1 - \bar{\Omega}_1, \Omega_2 - \bar{\Omega}_2, \dots)^2 = ((\Omega_1 - \bar{\Omega}_1)^2, (\Omega_2 - \bar{\Omega}_2)^2, \dots),$$

wo $\bar{\Omega}_k$ die relative Konjugierte der ganzen algebraischen Zahl Ω_k ist. Folglich ist $\mathfrak{d} \mid D$. Da D' im Körper $k(\sqrt{-q})$ quadratfrei ist, so kann die Zahl $\frac{m\sqrt{D}}{g}$ mit ganzen m und g (das Lösung der Gleichung $g^2 x^2 = m^2 D$ ist), dann und nur dann eine ganze algebraische Zahl sein, wenn $g = m\varepsilon, 2m\varepsilon$, ε Einheit. Nun ist die Zahl $\frac{1 + \sqrt{D'}}{2}$, der Gleichung $4x^2 - 4x = D' - 1$ gemäß, dann und nur dann ganz, wenn $D' \equiv 1 \pmod 4$ ist. Also ist für $D' \not\equiv 1 \pmod 4$ jede Zahl $\alpha + \beta\sqrt{D'}$ im Körper $K(\sqrt{D})$ dann und nur dann ganz, wenn α, β ganze Zahlen des Körpers $k(\sqrt{-q})$ sind (denn $2\alpha, 2\beta$ sind ganz und es ist $4\alpha^2 \equiv D\beta^2 \pmod 4$). Demnach ist $\mathfrak{d} = D'$ für $D' \equiv 1 \pmod 4$ und $\mathfrak{d} = D$ für $D' \not\equiv 1 \pmod 4$.

Definition 3. Die Menge aller binären quadratischen Formen $\varepsilon ax^2 + bxy + \varepsilon^{-1} cy^2$, wo ε eine beliebige Einheit des Körpers k ist und $ax^2 + bxy + cy^2$ zu einer bestimmten Klasse C gehört, werden wir als Hyperklasse bezeichnen.

Nun können wir den Idealklassen eines relativ-quadratischen Körpers $K(\sqrt{D})$, wo $\frac{D}{4}$ im Grundkörper k quadratfrei ist, die binären quadratischen Formen mit Koeffizienten aus k zuordnen. Ist nämlich $\mathfrak{P}$ ein Primideal des relativ-quadratischen Körpers $K(\sqrt{D})$, das kein Primideal des Körpers k ist, so kann $\mathfrak{P}$ in der Form $\left(\mathfrak{p}, \frac{\alpha + \sqrt{D}}{2}\right)$

dargestellt werden, wo α ein Ideal, $\mathfrak{p}$ ein Primideal des Körpers k ist (vgl. Hilbert S. 377; dort ist dies nur für $(\mathfrak{P}, 2D) = 1$ durchgeführt, man kann dies aber ganz analog auch für $\mathfrak{P}|2D$ beweisen). Diesem Ideale kann eine Hyperklasse von binären quadratischen Formen zugeordnet werden. Ist nämlich D die Relativdiskriminante des Körpers $K(\sqrt{D})$, so ordnen wir dem Ideale $\left(\mathfrak{p}, \frac{\alpha + \sqrt{D}}{2}\right)$ die Formen $\mathfrak{p}x^2 + \alpha xy + \frac{\alpha^2 - D}{4\mathfrak{p}} y^2$ zu. Da jedes Ideal Produkt von endlich vielen Primidealen ist, so kann man jedem Ideale (das einen Primidealteiler vom Typus $\left(\mathfrak{p}, \frac{\alpha + \sqrt{D}}{2}\right)$ hat) eine Form zuordnen, nämlich das symbolische Produkt der Formen, welche den Idealen $\left(\mathfrak{p}, \frac{\alpha + \sqrt{D}}{2}\right)$ entsprechen.

Um zu beweisen, daß diese Zuordnung eindeutig ist, betrachten wir die Ideale

$$\mathfrak{a}_1 = \left[a_1, \frac{-b_1 + \sqrt{D}}{2}\right], \qquad \mathfrak{a}_2 = \left[a_2, \frac{-b_2 + \sqrt{D}}{2}\right],$$

wo $a_1 = N(\mathfrak{a}_1)$, $a_2 = N(\mathfrak{a}_2)$ die Relativnormen von $\mathfrak{a}_1$ und $\mathfrak{a}_2$ sind. Also sind a_1 und b_1 Idealzahlen des Grundkörpers k, und es ist $N(\mathfrak{a}_1\mathfrak{a}_2) = a_1a_2$, ferner

$$\mathfrak{a}_1\mathfrak{a}_2 = \left[a_1a_2, a_1\frac{-b_2+\sqrt{D}}{2}, a_2\frac{-b_1+\sqrt{D}}{2}, \frac{b_1b_2 + D - (b_1+b_2)\sqrt{D}}{4}\right].$$

Wollen wir die zweigliedrige Basis von $\mathfrak{a}_1\mathfrak{a}_2$ berechnen, so verfahren wir etwas allgemeiner, als es z. B. Cahen S. 702–712 tut. Wir setzen nämlich

$$\delta = \left(a_1, a_2, \frac{b_1 + b_2}{2}\right), \qquad \delta = a_1x + a_2y + \frac{b_1 + b_2}{2}z,$$

wo x, y, z gewisse Idealzahlen von k sind. Offenbar ist auch

$$\delta \mid \frac{b_1b_2 + D}{2},$$

und demnach kann man setzen

$$\frac{-\left(a_1b_2x + a_2b_1y + \frac{b_1b_2 + D}{2}z\right) + \delta\sqrt{D}}{2} = \delta\frac{-b + \sqrt{D}}{2},$$

wo b eine gewisse Idealzahl ist. Somit ergibt sich, da $N(\mathfrak{a}_1\mathfrak{a}_2) = \delta^2\frac{a_1a_2}{\delta^2}$ ist,

$$\mathfrak{a}_1\mathfrak{a}_2 = \delta\left[\frac{a_1a_2}{\delta^2}, \frac{-b+\sqrt{D}}{2}\right],$$

$$\left(a_1x_1 + \frac{b_1 - \sqrt{D}}{2}y_1\right)\left(a_2x_2 + \frac{b_2 - \sqrt{D}}{2}y_2\right) = \delta\left(aX + \frac{b - \sqrt{D}}{2}Y\right),$$

wo

$$a = \frac{a_1a_2}{\delta^2}, \quad \delta Y = a_1x_1y_2 + a_2x_2y_1 + \frac{b_1 + b_2}{2}y_1y_2,$$

$$a\delta X = a_1a_2x_1x_2 + \frac{a_1(b_2 - b)\,x_1y_2 + a_2\,(b_1 - b)\,x_2y_1}{2} + \frac{b_1b_2 + D - b\,(b_1 + b_2)}{4}y_1y_2.$$

Mithin ist symbolisch

$$(a_1x_1^2 + b_1x_1y_1 + c_1y_1^2)\,(a_2x_2^2 + b_2x_2y_2 + c_2y_2^2) = aX^2 + bXY + cY^2,$$

wo $D = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2 = b^2 - 4ac$ ist. Demnach entspricht dem Produkte zweier Ideale das Produkt der zugeordneten Formen. Jetzt können wir, wie bei J. Sommer [4])

[4]) J. Sommer, Vorlesungen über Zahlentheorie, Leipzig und Berlin 1907, S. 218/19.

beweisen, daß wenn zwei Ideale zur selben Klasse gehören, die entsprechenden Formen äquivalent sind. Wollen wir also die Klassenzahl der binären quadratischen Formen $ax^2 + bxy + cy^2$ bestimmen, wo $b^2 - 4ac = D$ die Relativdiskriminante eines relativquadratischen Körpers ist und a, b, c Idealzahlen des Grundkörpers k sind, so genügt es, die Anzahl der Idealklassen zu berechnen. Wir können hier also die Herglotzsche Formel [1]) anwenden. Nehmen wir aber nur ganze algebraische Zahlen a, b, c, so können wir nicht die Herglotzsche Formel anwenden. Es gilt nämlich der folgende

Satz 1. *Die Klassenzahl H der binären quadratischen Formen mit der Determinante $4D$, wo $D \not\equiv -1 \pmod 4$ eine quadratfreie natürliche Zahl ist, deren Koeffizienten ganze Zahlen aus dem Körper $K(\sqrt{-q})$ mit primzahligem $q \equiv -1 \pmod 4$ sind, ist kein Vielfaches der Klassenzahl h des Körpers $K(\sqrt{-q})$, wenn nur h relativ prim zur Klassenzahl von $K(\sqrt{D})$ und von $K(\sqrt{-Dq})$ ist und $(D, q) = 1$.*

Beweis. Es sei h_1 die Klassenzahl von $K(\sqrt{D})$, $D \equiv -1 \pmod 4$, h die von $K(\sqrt{-q})$, und h_2 die von $K(\sqrt{-Dq})$, ferner g ein Primteiler von h. Wir wollen beweisen, daß H nicht durch g teilbar ist. Es sei nämlich C^g, wo C eine Idealklasse des relativquadratischen Körpers $K(\sqrt{D}, \sqrt{-q})$ bezeichnet, die Einheitsklasse. Nach einem Furtwänglerschen Satz [5]) befinden sich in der Idealklasse C unendlich viele Primideale. Es sei z. B. $\mathfrak{p}$ ein solches Primideal, das zur Diskriminante von $K(\sqrt{D}, \sqrt{-q})$ relativ prim ist. Ist $\mathfrak{p}$ kein Hauptideal des Körpers $K(\sqrt{-q})$, so führen wir in $\mathfrak{p}$ die Transformation $(\sqrt{D}: -\sqrt{D})$ durch. Ist $\mathfrak{p}'$ das neuentstandene Ideal, so ergibt sich, daß $\mathfrak{P} = \mathfrak{p}\mathfrak{p}'$ ein zum Körper $K(\sqrt{-q})$ gehöriges Primideal ist. Ist $F = ax^2 + bxy + cy^2$ die Form, die der Klasse C entspricht, so ergibt sich, daß in $K(\sqrt{-q})$ eine Primidealzahl P (relative Norm von $\mathfrak{p}$), für die $\mathfrak{P} | P$, durch F darstellbar ist. Aus der symbolischen Gleichung $F^g = x^2 - Dy^2$ folgt, für gewisse u, v, daß $\varepsilon P^g = u^2 - Dv^2$, $(u, v) = 1$, und damit auch $\bar{\varepsilon}\bar{P}^g = \bar{u}^2 - D\bar{v}^2$ ist, wo ε ideale Einheit und $\bar{x}$ die Konjugierte von x in $K(\sqrt{-q})$ bezeichnet. Somit erhalten wir

$$(1) \qquad p^g = (P\bar{P})^g = (u\bar{u} \mp Dv\bar{v})^2 - D(u\bar{v} \mp v\bar{u})^2,$$

wo $p = P\bar{P}$ eine rationale Primzahl ist, wenn nur $(P, \bar{P}) = 1$, für die p^g durch die Form $x^2 - Dy^2$ und auch durch die Form $x^2 + Dqy^2$ mit ganzen rationalen x, y darstellbar ist (die Zahl $\dfrac{u\bar{v} - v\bar{u}}{\sqrt{-q}}$ ist nämlich ganz und rational). Nun ist offenbar $(u\bar{v} + \varepsilon v\bar{u}, p) \neq 1$, $\varepsilon = \pm 1$; sonst würde sich aus $\dfrac{u}{v} \equiv \pm \dfrac{\bar{u}}{\bar{v}} \pmod p$ ergeben, daß $P | \bar{P}$.

Aus $(g, h_1 h_2) = 1$ folgt, daß p durch die Form $x^2 - Dy^2$ und auch durch die Form $x^2 + Dqy^2$ mit rationalen x, y darstellbar ist. Die Zahl p ist also im Körper $K(\sqrt{-q})$ durch die Form $x^2 - Dy^2$ zweimal darstellbar; vgl. Hilfssatz 2 des zweiten Teiles und [6]) S. 323. Demnach ist P^2, wie auch $\bar{P}^2$ durch die Form $x^2 - Dy^2$ im Körper $K(\sqrt{-q})$ eigentlich darstellbar [6]). Wegen der eigentlichen Darstellbarkeit von P^g durch die Form $x^2 - Dy^2$ in $K(\sqrt{-q})$, muß ebenso P durch diese Form in $K(\sqrt{-q})$ eigentlich darstellbar sein.

---

[5]) Ph. Furtwängler, Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers, Math. Ann. **63** (1907), S. 37.

[6]) S. Lubelski, Beweis und Verallgemeinerung eines Waring-Legendreschen Satzes, Math. Zeitschr. **33** (1931), S. 337, Satz 4.

Da P eine Primidealzahl ist, so kann sie durch keine anderen Formen der Determinante D darstellbar sein. Die Klasse C muß also Hauptklasse sein*), und somit ist $(g, H) = 1$.

Wir heben jetzt diejenige Gruppe von Idealklassen hervor, die den binären quadratischen Formen mit ganzen Koeffizienten aus $K(\sqrt{-q})$ entspricht.

Definition 4. Eine binäre quadratische Form der Determinante D mit Koeffizienten, die ganze Zahlen aus $K(\sqrt{-q})$ sind, werden wir eine reale (binäre quadratische) Form nennen.

Definition 5. Eine Idealklasse des relativ-quadratischen Körpers $\Re(\sqrt{D})$, der eine reale binäre quadratische Form entspricht, werden wir reale Idealklasse nennen. Enthält eine solche Idealklasse mindestens ein Ideal, das durch kein zu $K(\sqrt{-q})$ gehöriges Ideal teilbar ist, so werden wir sie primitive Idealklasse nennen.

Wir haben oben eine eineindeutige Zuordnung zwischen den Idealklassen des relativ-quadratischen Körpers $\Re(\sqrt{D})$ und den Klassen der binären quadratischen Formen festgesetzt. Es entsteht also die Frage: Wann entspricht einer Idealklasse eine reale Form? Einen Beitrag zur Beantwortung dieser Frage bietet der folgende Satz:

Satz 2. *Einer primitiven realen Idealklasse entspricht eine primitive reale binäre quadratische Form und umgekehrt entspricht einer solchen Form eine reale primitive Idealklasse.*

Beweis. Es sei $ax^2 + bxy + cy^2$ eine reale Form, die in bezug auf $K(\sqrt{-q})$ primitiv ist, d. h. a habe keinen gemeinsamen Idealteiler mit b und c. Nach Hilfssatz 2 existiert eine zu $ax^2 + bxy + cy^2$ äquivalente Form $a_1x^2 + b_1xy + c_1y^2$, für die $(a_1, 2D) = 1$ und a_1, b_1, c_1 ganze Zahlen von $K(\sqrt{-q})$ sind. Nun folgt aus

$$a_1(a_1x^2 + b_1xy + c_1y^2) = \left(a_1x + \frac{b_1 + \sqrt{D}}{2}y\right)\left(a_1x + \frac{b_1 - \sqrt{D}}{2}y\right),$$

daß das Ideal $\left[a_1, \frac{b_1 + \sqrt{D}}{2}\right]$ durch kein zu $K(\sqrt{-q})$ gehöriges Ideal teilbar ist. Wäre nämlich $\mathfrak{d}$ ein solches Ideal, so würde sich aus $\mathfrak{d}|a_1$, $\mathfrak{d}|b_1$ und $\mathfrak{d}^2|D$ ergeben, daß $(a_1, 2D) \neq 1$ ist, was der Annahme widerspricht.

Umgekehrt sei jetzt j ein Ideal, dessen relative Norm eine ganze algebraische Zahl ist. Nun kann bekanntlich die Basis von j als zweigliedrig angenommen werden, wobei ein Glied bis auf die Zugehörigkeit zu j beliebig angenommen werden kann. Es sei dieses Glied gleich der relativen Norm von j, also eine ganze algebraische Zahl a von $K(\sqrt{-q})$. Man setze als zweites Basisglied $u + v\omega$, wo $\omega = \sqrt{D}$ resp. $\omega = \frac{1 + \sqrt{D}}{2}$. Da j durch kein zu $K(\sqrt{-q})$ gehöriges Ideal teilbar ist, so haben u und v mit j keinen Teiler gemeinsam, und mithin ist die Kongruenz $v \equiv Bu \pmod{a}$ lösbar, woraus folgt, daß $B + \omega \equiv 0 \pmod{j}$ ist. Damit erhalten wir eine reale primitive binäre quadratische Form $ax^2 + Bxy + \frac{B^2 - D}{4a}y^2$, die dem Ideale j entspricht.

Folgerung. *Die realen primitiven Idealklassen bilden eine Gruppe.*

Der Beweis folgt unmittelbar aus der Tatsache, daß wenn jeder Faktor eines Produkts durch kein zu $K(\sqrt{-q})$ gehöriges Ideal teilbar ist, auch das Produkt diese Eigenschaft hat, wenn nur die Faktoren keine relativ-konjugierten Teiler haben. Ferner gilt dies, da die relative Norm jedes Faktors eine ganze Zahl aus $K(\sqrt{-q})$ ist, auch für die Norm des Produktes. Nach Satz 2 ist damit die Folgerung bewiesen.

*) Ist $P|\overline{P}$, ist also P einer rationalen Primzahl P_1 in $K(\sqrt{-q})$ assoziiert, so folgt aus (1), daß $P_1^2 = x^2 - Dy^2$ bzw. $= x^2 + Dqy^2$, wo x, y natürliche Zahlen bezeichnen. Demnach ist $C^2 = C^g =$ Einheitsklasse $= E$.

In gewissen Fällen kann man leicht aus den realen Idealklassen sämtliche Idealklassen eines relativ-quadratischen Körpers $\mathfrak{R}(\sqrt{D})$ erhalten. Es gilt nämlich der folgende Satz:

Satz 3. *Ist h_1 resp. h_2 resp. h die Klassenzahl des quadratischen Körpers $K(\sqrt{D})$ resp. $K(\sqrt{-Dq})$ resp. $K(\sqrt{-q})$, $q \geqq 3$, und $(h, \frac{1}{2}h_1h_2) = 1$, so ist jede reale primitive Idealklasse h-te Potenz einer Klasse des relativ-quadratischen Körpers $\mathfrak{R}(\sqrt{D})$.*

Beweis. Es bezeichne

$$C_1^h, C_2^h, \ldots, C_n^h \tag{1}$$

die Folge sämtlicher verschiedener h-ter Potenzen der Idealklassen von $\mathfrak{R}(\sqrt{D})$. Jede Klasse von (1) stellt eine reale primitive Idealklasse dar. Wir erhalten nämlich aus $N(j)^h = g$, wo $N(j)$ die relative Norm von j bezeichnet, daß g eine ganze Zahl aus $K(\sqrt{-q})$ ist. Ferner ist jede solche von der Hauptklasse von $K(\sqrt{-q})$ verschiedene Idealklasse primitiv. Denn gehört C_i^h nicht zur Hauptklasse von $K(\sqrt{-q})$, so gehört das in C_i^h existierende Primideal $\mathfrak{P}$ nicht zu $K(\sqrt{-q})$. Wir wollen jetzt beweisen, daß in der Folge (1) sämtliche realen primitiven Idealklassen enthalten sind. Denn sind

$$K_1, K_2, \ldots, K_t \tag{2}$$

sämtliche primitiven realen Idealklassen von $\mathfrak{R}(\sqrt{D})$, so ist die Folge

$$K_1^h, K_2^h, \ldots, K_t^h \tag{3}$$

von (2) nicht verschieden. Den Idealklassen (2) entsprechen nämlich reale binäre primitive quadratische Formen. Nach dem Hauptsatze dieser Arbeit (s. Teil 2) ist diese Klassenzahl gleich $\frac{1}{2}h_1h_2$, wo h_1 die Klassenzahl von $K(\sqrt{D})$ und h_2 die von $K(\sqrt{-Dq})$, $q \geqq 3$, bezeichnet. Da $(h, \frac{1}{2}h_1h_2) = 1$ ist, so kann dann und nur dann $K_1^h = K_2^h$ sein, wenn $K_1 = K_2$ ist. Demnach ist die Folge (3) mit der Folge (2), von der Reihenfolge abgesehen, identisch.

Folgerung. *Unter denselben Voraussetzungen wie in Satz 3 und im Hauptsatz dieser Arbeit ist $\frac{1}{2}hh_1h_2 \mid H$.*

Beweis. Nach Satz 3 (s. auch seinen Beweis) genügt es zu beweisen, daß die Gleichung $x^h = 1$ in der Idealklassengruppe von $\mathfrak{R}(\sqrt{D})$ h Wurzeln hat. Dies ist evident. Denn sind die Klassen der Ideale j_1 und j_2 in $K(\sqrt{-q})$ verschieden, so sind sie es auch in $\mathfrak{R}(\sqrt{D})$.

Zweiter Teil.

In diesem Teile werden wir eine genaue Formel für den Fall angeben, wo die Koeffizienten ganze algebraische Zahlen sind. Zu betonen ist, daß die Überlegungen dieses Teiles vom ersten Teil, bis auf die Hilfssätze 2 und 5, unabhängig sind.

Hilfssatz 1. *Jede Transformation in sich* (oder jede automorphe Transformation)

$$x = \varkappa x' + \lambda y', \quad y = \mu x' + \nu y', \quad \varkappa\nu - \lambda\mu = 1 \tag{1}$$

einer binären quadratischen Form $f(x, y) = ax^2 + bxy + cy^2$, $(a, b, c) = 1$, wobei a, b, c ganze Zahlen des algebraischen Körpers $K(\theta)$ sind und $\sqrt{b^2 - 4ac}$ kein Element dieses Körpers ist, kann in diesem Körper durch die Matrix

$$\begin{pmatrix} \frac{t - bu}{2} & -cu \\ au & \frac{t + bu}{2} \end{pmatrix} \tag{2}$$

dargestellt werden, wo t und u ganze Zahlen des Körpers $K(\theta)$ sind, für die $t^2 - (b^2 - 4ac)u^2 = 4$ ist.

Beweis. Jede Transformation der Form $f(x, y)$ in sich im Körper $K(\theta)$ ist auch eine Transformation der Form

$$af(x, y) = a(ax^2 + bxy + cy^2) = \left(ax + \frac{b + \sqrt{D}}{2} y\right)\left(ax + \frac{b - \sqrt{D}}{2} y\right)$$

in sich, wo $D = b^2 - 4ac$ ist. Es bezeichne

$$M = \frac{b + \sqrt{D}}{2}, \qquad \overline{M} = \frac{b - \sqrt{D}}{2}.$$

Da $\begin{pmatrix} \varkappa & \lambda \\ \mu & \nu \end{pmatrix}$ eine automorphe Transformation der Form $f(x, y)$ ist, so muß

$$(3) \qquad f(\varkappa, \mu) = a, \quad f(\lambda, \nu) = c, \quad 2a\varkappa\lambda + b(\varkappa\nu + \lambda\mu) + 2c\mu\nu = b,$$

$$(4) \quad af(x, y) = [(a\varkappa + M\mu)\, x + (a\lambda + M\nu)y][(a\varkappa + \overline{M}\mu)\, x + (a\lambda + \overline{M}\nu)y]$$

sein. Da $a\left(x^2 + \frac{a}{b} x + \frac{c}{a}\right)$ im relativ-quadratischen Körper $\mathfrak{K}(\sqrt{D})$ eindeutig in normierte lineare Faktoren zerfällt, so ist nach (3)

$$\frac{a\lambda + M\nu}{a\varkappa + M\mu} = \frac{(a\lambda + M\nu)(a\varkappa + \overline{M}\mu)}{(a\varkappa + M\mu)(a\varkappa + \overline{M}\mu)} = \frac{a^2\lambda\varkappa + aM\nu\varkappa + a\lambda\overline{M}\mu + M\overline{M}\nu\mu}{af(\varkappa, \mu)}$$

$$= \frac{2a\varkappa\lambda + b(\varkappa\nu + \lambda\mu) + 2c\mu\nu + \sqrt{D}\,(\varkappa\nu - \lambda\mu)}{2f(\varkappa, \mu)} = \frac{b + \sqrt{D}}{2a},$$

und mithin ist für eine gewisse Zahl ε des relativ-quadratischen Körpers $\mathfrak{K}(\sqrt{D})$

$$(5) \qquad a\lambda + M\nu = \varepsilon M, \qquad a\varkappa + M\mu = \varepsilon a.$$

Nach Gleichung (4) muß also ε eine relative Einheit des relativ-quadratischen Körpers $\mathfrak{K}(\sqrt{D})$ sein. Wir wollen jetzt beweisen, daß man solche ganze Zahlen t, u des Körpers $K(\theta)$ finden kann, für die

$$\varepsilon = \frac{t + u\sqrt{D}}{2}, \qquad t^2 - Du^2 = 4$$

ist. Man erhält nämlich aus (5)

$$\varepsilon = \varkappa + \mu\frac{M}{a} = \nu + \lambda\frac{a}{M}.$$

Ist $\bar{\varepsilon}$ die Konjugierte von ε im relativ-quadratischen Körper $\mathfrak{K}(\sqrt{D})$, so ist

$$\bar{\varepsilon} = \varkappa + \mu\frac{\overline{M}}{a} = \nu + \lambda\frac{a}{\overline{M}}.$$

Daraus ergibt sich

$$(\varepsilon - \bar{\varepsilon})^2 = \mu^2\frac{(M - \overline{M})^2}{a^2} = \mu^2\frac{D}{a^2} = \lambda^2 a^2\frac{(\overline{M} - M)^2}{M^2\overline{M}^2} = \lambda^2\frac{D}{c^2}.$$

Da $(a, b, c) = 1$ ist, so muß auch $(D, a, c) = 1$ sein, und es folgt daraus, daß $\varepsilon - \bar{\varepsilon} = u\sqrt{D}$, wo u eine gewisse ganze Zahl des Körpers $K(\theta)$ ist. Somit ist für eine gewisse Zahl t des Körpers $K(\theta)$

$$\varepsilon = \frac{t + u\sqrt{D}}{2}, \quad \bar{\varepsilon} = \frac{t - u\sqrt{D}}{2}, \quad \varepsilon\bar{\varepsilon} = \frac{t^2 - Du^2}{4} = 1.$$

Es ist also auch t ganz. Setzen wir jetzt in den Gleichungen (4) für ε den Wert $\frac{t + u\sqrt{D}}{2}$

ein, so erhalten wir aus den Gleichungen

$$a\lambda + M\nu = \varepsilon M, \qquad a\lambda + \overline{M}\nu = \bar{\varepsilon}\overline{M}$$

die Werte von $\varkappa$, μ, λ, ν, die durch die Matrix (2) angegeben sind.

Bemerkung. A. Speiser [7]) fand für jede automorphe Transformation die folgende Matrix:

$$\begin{pmatrix} \frac{t + \mathfrak{b}u}{2} & \frac{\mathfrak{u}}{\mathfrak{m}} MSM \\ \frac{-\mathfrak{u}}{\mathfrak{m}} aSa & \frac{t - \mathfrak{b}u}{2} \end{pmatrix},$$

wobei $\mathfrak{u}$, $\mathfrak{m}$, $\mathfrak{b}$ gewisse Ideale sind und Sx die Konjugierte von x bezeichnet.

Bezeichnung 1. In einem quadratischen Körper $K(\sqrt{-q})$ werden wir mit $\bar{z} = \frac{a - b\sqrt{-q}}{2}$ stets die Konjugierte der Zahl $z = \frac{a + b\sqrt{-q}}{2}$ bezeichnen.

Hilfssatz 2. *Die Pellsche Gleichung $x^2 - Dy^2 = 4$, wo $D > 1$ eine natürliche Zahl ist, hat im Bereiche der ganzen Zahlen eines beliebigen imaginär-quadratischen Körpers $K(\sqrt{-q})$ mit $q \geqq 3$ nur ganze rationale Lösungen.*

Im Gaußschen Körper sind die Lösungen für $D \neq 1, 3$ entweder ganz und rational oder rein imaginär.

Beweis. Es seien t, u ganze Zahlen eines imaginär-quadratischen Körpers $K(\sqrt{-q})$, für die $t^2 - Du^2 = 4$ ist. Also ist auch $\bar{t}^2 - D\bar{u}^2 = 4$. Multiplizieren wir diese Gleichungen miteinander, so ist nach der Eulerschen Identität

$$(6) \qquad (t\bar{t} + \varepsilon Du\bar{u})^2 - D(t\bar{u} + \varepsilon u\bar{t})^2 = 16, \qquad \varepsilon = \pm 1.$$

Setzen wir

$$t\bar{t} - Du\bar{u} = a, \qquad t\bar{u} - tu = b\sqrt{-q},$$

so ergibt sich, daß a und b ganze rationale Zahlen sind, wobei b für $q \not\equiv -1 \bmod 4$ gerade ist. Wir haben also $a^2 + Dqb^2 = 16$, wo Dq nach Voraussetzung eine natürliche Zahl ist. Somit kann entweder

$$a^2 = b^2 = 1, \quad Dq = 15 \quad \text{oder} \quad a^2 = 4, \quad Dqb^2 = 12 \quad \text{oder} \quad b = 0$$

sein. Im ersten Falle kann nicht $q = 1$ oder $q = 5$ sein, denn aus $2 \mid b$ folgt $Dqb^2 > 16$. Es kann also höchstens $D = 5$, $q = 3$ sein, und somit ergibt sich aus Gleichung (6), für $\varepsilon = 1$, da $-D \equiv 3 \pmod 8$, daß $t\bar{t} + Du\bar{u}$ gerade sein muß (andernfalls wäre die linke Seite der Gleichung (6), für $\varepsilon = 1$, kongruent 4 (mod 8)). Demnach muß auch die Zahl $a = t\bar{t} - Du\bar{u}$ und mithin auch $b = \frac{t\bar{u} - \bar{t}u}{\sqrt{-q}}$ durch 2 teilbar sein, was offenbar unmöglich ist.

Im zweiten Falle kann, da nach Voraussetzung $Dq > 3$, nur $q = 3$, $D = 4$ sein, und $t\bar{u} + \bar{t}u$ muß, da $D(t\bar{u} + \bar{t}u)^2$ Quadratzahl ist, ebenfalls gerade sein (sogar $= 0$). Mithin ist auch $t\bar{u} - \bar{t}u$ durch 2 teilbar, was unmöglich ist.

Es ist also der Satz noch für den Fall $b = 0$ zu beweisen. Offenbar ergibt sich aus $t^2 - Du^2 = \bar{t}^2 - D\bar{u}^2 = 4$, daß

$$(t, u) = \alpha, \quad (\bar{t}, \bar{u}) = \bar{\alpha}$$

---

[7]) A. Speiser, Die Theorie der binären quadratischen Formen mit Koeffizienten und Unbestimmten in einem beliebigen Zahlkörper, Diss. Göttingen 1909, S. 111.

ist, wo α ein Idealteiler von 2 ist (man kann $\alpha = 1, = 1 + i$ oder $= 2$ annehmen). Demnach folgt aus $t\bar{u} = \bar{t}u$ für ein gewisses ε

$$\bar{u} = \varepsilon u, \quad \bar{t} = \varepsilon t.$$

Somit ist

$$\bar{t}^2 - D\bar{u}^2 = \varepsilon^2(t^2 - Du^2) = 4, \quad \varepsilon^2 = 1.$$

Es muß also $\varepsilon = \pm 1$ sein. Nun sind für $\varepsilon = 1$ die Zahlen u, t ganz und rational. Für $\varepsilon = -1$ sind diese Zahlen rein imaginär, und es existieren demnach ganze rationale Zahlen u_1, t_1, für die $u = \sqrt{-q}\,u_1$, $t = \sqrt{-q}\,t_1$ ist. Nun ergibt sich aus

$$t^2 - Du^2 = -q(t_1^2 - Du_1^2) = 4,$$

daß dies nur für $q = 1$ möglich ist.

Von jetzt ab machen wir die folgenden Einschränkungen bezüglich des Körpers $K(\sqrt{-q})$ und der Determinante D der binären quadratischen Formen:

Bezeichnung 2. Mit $D > 4$ bezeichnen wir stets eine natürliche Zahl, für welche $\frac{D}{4} = D'$ im Körper $K(\sqrt{-q})$ ganz und quadratfrei ist. Ist $q = 1$, so sei noch $D' > 3$.

Definition 1. In einem imaginär-quadratischen Körper $K(\sqrt{-q})$ mit ungerader Klassenzahl sollen alle Formen $ax^2 + bxy + cy^2$ der Determinante $D = b^2 - 4ac > 1$, wo a, b, c ganze rationale Zahlen sind, $\frac{D}{4}$ im Körper $K(\sqrt{-q})$ quadratfrei und $D' > 3$ ist für $q = 1$, als Formen des ersten Typus bezeichnet werden.

Alle Formen derselben Determinante D von der Gestalt $a_1x^2 + b_1\sqrt{-q}xy + c_1y^2$, wo a_1, b_1, c_1 ebenfalls ganze rationale Zahlen sind, sollen Formen des zweiten Typus heißen.

Satz 1. *Sind zwei Formen des ersten Typus im imaginär-quadratischen Körper $K(\sqrt{-q})$ eigentlich resp. uneigentlich äquivalent, so sind sie für $q \geqq 3$ auch im rationalen Körper eigentlich resp. uneigentlich äquivalent. Ist $q = 1$, $D' > 3$, so ist eine Form $ax^2 + bxy + cy^2$ der Form $a_1x^2 + b_1xy + c_1y^2$ (beide vom ersten Typus) eigentlich resp. uneigentlich äquivalent, wenn im rationalen Körper die Form $ax^2 + bxy + cy^2$ der Form $a_1x^2 + b_1xy + c_1y^2$ oder der Form $-a_1x^2 + b_1xy - c_1y^2$ eigentlich resp. uneigentlich äquivalent ist.*

Beweis. Es sei

$$x = \alpha\xi + \beta\eta, \quad y = \gamma\xi + \delta\eta, \quad \alpha\delta - \beta\gamma = \pm 1, \tag{7}$$

wo $\alpha, \beta, \gamma, \delta$ ganze Zahlen des imaginär-quadratischen Körpers $K(\sqrt{-q})$ sind, die Transformation, mittels welcher die Form $f(x, y) = ax^2 + bxy + cy^2$ in die Form $f_1(x, y) = a_1x^2 + b_1xy + c_1y^2$ übergeht. Es ist also

$$a_1 = f(\alpha, \gamma), \; c_1 = f(\beta, \delta), \; b_1 = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta. \tag{8}$$

Der Transformation (7) gemäß erhält man

$$f(\bar{\alpha}, \bar{\gamma}) = a_1, \quad f(\bar{\beta}, \bar{\delta}) = c_1, \quad 2a\bar{\alpha}\bar{\beta} + b(\bar{\alpha}\bar{\delta} + \bar{\gamma}\bar{\beta}) + 2c\bar{\gamma}\bar{\delta} = b_1$$

(da die Zahlen a_1, b_1, c_1; a, b, c ganz und rational sind und $\bar{x}$ die Konjugierte von x ist). Dies ergibt, daß $\begin{pmatrix} \bar{\alpha} & \bar{\beta} \\ \bar{\gamma} & \bar{\delta} \end{pmatrix}$ ebenfalls eine eigentliche resp. uneigentliche Transformation ist, mittels der man die Form $f(x, y)$ in die Form $f_1(x, y)$ überführen kann. Ihre inverse Transformation ist also durch $\begin{pmatrix} \bar{\delta} & -\bar{\beta} \\ -\bar{\gamma} & \bar{\alpha} \end{pmatrix}$ dargestellt. Somit erhalten wir, daß

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \bar{\delta} & -\bar{\beta} \\ -\bar{\gamma} & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} \alpha\bar{\delta} - \beta\bar{\gamma} & -\alpha\bar{\beta} + \beta\bar{\alpha} \\ \gamma\bar{\delta} - \delta\bar{\gamma} & -\gamma\bar{\beta} + \delta\bar{\alpha} \end{pmatrix}$$

eine für die Form $ax^2 + bxy + cy^2$ automorphe Transformation ist.

Nach Hilfssatz 1 muß für gewisse t und u, für die $t^2 - Du^2 = 4$ ist,

$$(9)\quad \alpha\bar{\delta} - \beta\bar{\gamma} = \frac{t - bu}{2},\ -\alpha\bar{\beta} + \bar{\alpha}\beta = -cu,\ \gamma\bar{\delta} - \delta\bar{\gamma} = au,\ -\gamma\bar{\beta} + \delta\bar{\alpha} = \frac{t + bu}{2}$$

sein. Nach Hilfssatz 2 sind die Zahlen t, u für $D > 1$ entweder ganz und rational oder (was nur für $q = 1$, $D > 3$ möglich ist) rein imaginär. Da $\alpha\bar{\delta} - \beta\bar{\gamma}$, $\bar{\alpha}\delta - \gamma\bar{\beta}$ konjugierte Zahlen sind, so muß, falls u und t imaginär sind, $t - bu = -(t + bu)$ sein, was $t = 0$ und mithin $-Du^2 = 4$, $D = 4$ gibt. Da nach Voraussetzung $D > 4$ ist, so können wir also annehmen, daß t und u und demnach auch die linken Seiten der Gleichungen (9) ganze rationale Zahlen sind. Somit ist

$$\alpha\bar{\delta} - \beta\bar{\gamma} = \bar{\alpha}\delta - \beta\bar{\gamma},\quad \text{d. h.}\quad t - bu = t + bu\,,$$

also ist $bu = 0$. Man kann $u = 0$ setzen; denn ist $\beta\bar{\alpha} - \alpha\bar{\beta}$ reell, so muß es gleich 0 sein, also ist $u = 0$. (Andererseits läßt sich für $b = 0$ die Form $ax^2 + cy^2$ durch eine ihr im rationalen Körper äquivalente Form $Ax^2 + Bxy + Cy^2$ mit $B \neq 0$ ersetzen. Ist der Satz für diese Form bewiesen, so wird er es auch für $ax^2 + cy^2$ sein.) Aus $u = 0$ ergibt sich aber

$$-\alpha\bar{\beta} + \beta\bar{\alpha} = 0 \quad \text{und} \quad \gamma\bar{\delta} - \delta\bar{\gamma} = 0\,.$$

Man hat also für $\alpha\beta\gamma\delta \neq 0$, daß

$$(10)\qquad \frac{\alpha}{\beta} = \frac{\bar{\alpha}}{\bar{\beta}} = k,\quad \frac{\gamma}{\delta} = \frac{\bar{\gamma}}{\bar{\delta}} = k_1\,,$$

wo offenbar k und k_1 rationale Zahlen sind. Setzt man $k = \frac{r}{s}$, $(r, s) = 1$, wo r und s ganze rationale Zahlen sind, so erhalten wir $r \mid \alpha$, $s \mid \beta$. Setzen wir $\alpha = \varepsilon r$, $\beta = \varepsilon s$, so ergibt sich, da $(\alpha, \beta) = 1$, daß ε eine Einheit sein muß. Ebenso folgt: sind r_1, s_1 ganze rationale Zahlen, für welche $k_1 = \frac{r_1}{s_1}$, $(r_1, s_1) = 1$ ist, so erhält man für eine ganze Einheit ε_1, daß $\gamma = \varepsilon_1 r_1$, $\delta = \varepsilon_1 s_1$ ist. Nun sind für $q > 3$ alle Einheiten des Körpers $K(\sqrt{-q})$ gleich ± 1, demnach müssen $\alpha, \beta, \gamma, \delta$ für $q > 3$ ganze rationale Zahlen sein. Man kann also $\alpha\beta\gamma\delta = 0$ für $q > 3$ annehmen. Da $\alpha\delta - \beta\gamma = \pm 1$ ist, muß entweder $\alpha\delta = \pm 1$ oder $-\beta\gamma = \pm 1$ sein, woraus entweder

$$\alpha = \pm 1,\quad \delta = \pm 1 \quad \text{oder} \quad \beta = \pm 1,\quad \gamma = \pm 1$$

folgt. Nun ergibt sich aus den Gleichungen (10), daß mit α auch β (resp. mit β auch α) ganz und rational sein muß. Satz 1 ist also für $q > 3$ bewiesen.

Es sei jetzt $q = 1$ oder $q = 3$. Wir können die Matrix der Transformation (7) in der Form

$$\begin{pmatrix} \varepsilon r & \varepsilon s \\ \varepsilon_1 r_1 & \varepsilon_1 s_1 \end{pmatrix}$$

darstellen. Wir haben also

$$\alpha\delta - \beta\gamma = \varepsilon\varepsilon_1(rs_1 - r_1 s) = \pm 1\,.$$

Die ganzen rationalen Zahlen r, s, r_1, s_1 können so angenommen werden, daß $\alpha\delta - \beta\gamma = rs_1 - r_1 s$ wird. Demnach ist $\varepsilon\varepsilon_1 = 1$. Ist nun $q = 3$, so ist

$$a_1 = \varepsilon^2 a r^2 + b r r_1 + \varepsilon_1^2 c r_1^2,\ c_1 = \varepsilon^2 a s^2 + b s s_1 + \varepsilon_1^2 c s_1^2.$$

Da aber $\varepsilon, \varepsilon_1$ konjugiert, a, b, a_1, b_1 ganze rationale Zahlen und die imaginären Einheiten des Körpers $K(\sqrt{-3})$ sämtlich von der Form $\frac{\pm 1 \pm \sqrt{3}}{2}$ sind, so müssen die

Imaginärteile der letzten Gleichungen gleich 0 sein und

$$ar^2 = cr_1^2, \quad as^2 = cs_1^2.$$

Daraus folgt $s^2r_1^2 = s_1^2r^2$, $sr_1 = \pm rs_1$, was mit der Gleichung $rs_1 - sr_1 = \pm 1$ im Widerspruch steht (ist nämlich $sr_1 \pm rs_1 = 0$, so muß $rs_1 - r_1s$ gerade sein). Die Einheit ε muß also auch hier rational sein, d. h. es ist $\varepsilon = \pm 1$.

Wir betrachten jetzt den letzten Fall, $q = 1$. Ist $\varepsilon \neq \pm 1$, so muß $\varepsilon = \pm i$ sein, also ist $\varepsilon_1 = -\varepsilon$ und mithin

$$\begin{pmatrix} \varepsilon r & \varepsilon s \\ -\varepsilon r_1 & -\varepsilon s_1 \end{pmatrix} = \begin{pmatrix} r & -s \\ -r_1 & s_1 \end{pmatrix} \begin{pmatrix} \varepsilon & 0 \\ 0 & -\varepsilon \end{pmatrix}.$$

Es sei $gx^2 + kxy + ly^2$ die Form, in die $ax^2 + bxy + cy^2$ mittels der Transformation $\begin{pmatrix} r & -s \\ -r_1 & s_1 \end{pmatrix}$ übergeht. Transformieren wir die Form $gx^2 + kxy + ly^2$ mittels $\begin{pmatrix} \varepsilon & 0 \\ 0 & -\varepsilon \end{pmatrix}$, so erhalten wir die Form $-gx^2 + kxy - ly^2$. Es muß also entweder die Form $gx^2 + kxy + ly^2$ oder die Form $-gx^2 + kxy - ly^2$ mit $a_1x^2 + b_1xy + c_1y^2$ identisch sein, und zwar je nachdem $\varepsilon = \pm 1$ oder $\varepsilon = \pm i$ ist. Also ist im rationalen Körper die Form $ax^2 + bxy + cy^2$ entweder der Form $a_1x^2 + b_1xy + c_1y^2$ oder der Form $-a_1x^2 + b_1xy - c_1y^2$ eigentlich resp. uneigentlich äquivalent, je nachdem

$$ax^2 + bxy + cy^2 \text{ und } a_1x^2 + b_1xy + c_1y^2$$

im Körper $K(i)$ eigentlich resp. uneigentlich sind.

Anmerkung. Die letzte Variante des Beweises hat N. Tschebotareff in folgender scharfsinniger Weise auf beliebige quadratische Körper verallgemeinert:

Ist $\alpha = \varepsilon\alpha_1$, $\beta = \varepsilon\beta_1$, $\gamma = \varepsilon_1\gamma_1$, $\delta = \varepsilon_1\delta_1$, wo α_1, β_1, γ_1, δ_1 ganz und rational und ε, ε_1 Einheiten von $K(\sqrt{-q})$ sind, so hat die Form

(I) $\quad a\varepsilon^2(\alpha_1x + \beta_1y)^2 + b\varepsilon\varepsilon_1(\alpha_1x + \beta_1y)(\gamma_1x + \delta_1y) + c\varepsilon_1^2(\gamma_1x + \delta_1y)^2$

rationale Koeffizienten. Das gilt auch für die Form

$$a\varepsilon^2\xi^2 + b\varepsilon\varepsilon_1\xi\eta + c\varepsilon_1\eta^2$$

da sie aus (I) durch die rationale Transformation $\xi = \alpha_1x + \beta_1y$, $\eta = \gamma_1x + \delta_1y$ hervorgeht. Somit sind ε^2, $\varepsilon\varepsilon_1$, ε_1^2 rational, d. h. gleich ± 1. Unsere Transformation $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ kann nur im Falle $\varepsilon = \pm i$ oder $\varepsilon_1 = \pm i$ nicht rational sein, was nur für $q = 1$ möglich ist.

Satz 2. *Ist für $q \neq 2$ eine Form F vom ersten Typus im imaginär-quadratischen Körper $K(\sqrt{-q})$, von ungerader Klassenzahl einer Form vom zweiten Typus eigentlich äquivalent, so ist die Form F im rationalen Körper einer ambigen Form äquivalent. Für $q \geqq 3$ ist diese Bedingung auch hinreichend.*

Beweis. Wir wollen zunächst beweisen, daß die Bedingungen des Satzes dazu hinreichen, daß für $q \geqq 3$ eine Form vom ersten Typus einer Form vom zweiten Typus äquivalent sei. Es können nämlich alle im rationalen Körper ambigen Formen durch eine Form von der Gestalt

(11) $$Ax^2 + A\varrho xy + Cy^2, \quad \varrho = 0, 1$$

(s. z. B. Cahen S. 324—326) dargestellt werden. Ist die Form vom ersten Typus einer Form (11) mit $\varrho = 0$ äquivalent, so ist der Satz trivial (der mittlere Koeffizient der Form vom zweiten Typus kann als $0 \cdot \sqrt{-q}$ dargestellt werden). Es sei also $q \geqq 3$. Da $q \equiv -1 \pmod 4$ sein muß, so ist die Zahl $\frac{1 + \sqrt{-q}}{2}$ im Körper $K(\sqrt{-q})$ ganz. Nun geht

die Form $ax^2 + axy + cy^2$ mittels der Transformation $\begin{pmatrix} 1 & \frac{-1+\sqrt{-q}}{2} \\ 0 & 1 \end{pmatrix}$ in die Form $ax^2 + a\sqrt{-q}xy + \left(c - \frac{q+1}{4}a\right)y^2$ über.

Wir zeigen jetzt, daß die Bedingungen für $q \neq 2$ notwendig sind. Es seien $\alpha, \beta, \gamma, \delta$ ganze Zahlen aus dem Körper $K(\sqrt{-q})$, für die $\alpha\delta - \beta\gamma = 1$ und $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ die Transformation ist, die die Form $f(x, y) = ax^2 + bxy + cy^2$ in die Form $a_1x^2 + b_1\sqrt{-q}xy + c_1y^2$ verwandelt. Nach der Definition des Typus sind die Zahlen a, b, c; a_1, b_1, c_1 ganz und rational, und mithin bestehen auch die Gleichungen

$$f(\bar{\alpha}, \bar{\gamma}) = a_1, \quad f(\bar{\beta}, \bar{\delta}) = c_1, \quad 2a\bar{\alpha}\bar{\beta} + b(\bar{\alpha}\bar{\delta} + \bar{\gamma}\bar{\beta}) + 2c\bar{\gamma}\bar{\delta} = -b_1\sqrt{-q},$$

d. h. die Transformation $\begin{pmatrix} \bar{\alpha} & \bar{\beta} \\ \bar{\gamma} & \bar{\delta} \end{pmatrix}$ führt die Form $f(x, y)$ in $a_1x^2 - b_1\sqrt{-q}xy + c_1y^2$ über. Da zugleich $\bar{\alpha}\bar{\delta} - \bar{\beta}\bar{\gamma} = 1$ ist, so ergibt sich, daß die Formen

$$a_1x^2 + b_1\sqrt{-q}xy + c_1y^2, \quad a_1x^2 - b_1\sqrt{-q}xy + c_1y^2$$

eigentlich äquivalent sind. Demnach ist auch die Form $f(x, y)$ im Körper $K(\sqrt{-q})$ sich selbst uneigentlich äquivalent. Nach Satz 1 ist $f(x, y)$ im rationalen Körper ambig.

Hilfssatz 3. *Es seien N und L beliebige Zahlen eines beliebigen algebraischen Körpers $K(\theta)$ und $(2N, L) = 1$. Ferner sei L durch eine beliebige binäre quadratische Form der Determinante D eigentlich darstellbar. Ist $f(x, y) = ax^2 + bxy + cy^2$ eine beliebige binäre primitive quadratische Form (d. h. $(a, b, c) = 1$) der Determinante D, so existiert eine zu $f(x, y)$ eigentlich resp. uneigentlich äquivalente Form $Ax^2 + Bxy + Cy^2$, für die $L \mid A$ und $(A, N) = 1$ ist.*

Beweis. Nach Hilfssatz 2 des ersten Teils kann man ganze Zahlen x', y' des Körpers $K(\theta)$ so finden, daß $(f(x', y'), N) = 1$ ist. Da $(x', y', N) = 1$ und mit x' auch $x' + Nj^h$ eine Lösung ist, wo j sämtliche Primteiler von y' enthält, für die $(x', j) = 1$, und h die Klassenzahl von $K(\theta)$ bezeichnet, so kann $(x', y') = 1$ angenommen werden. Es seien jetzt ξ, η ganze Zahlen des Körpers $K(\theta)$ derart, daß $x'\eta - y'\xi = 1$ resp. $= -1$ ist. Die Transformation $\begin{pmatrix} x' & \xi \\ y' & \eta \end{pmatrix}$ führt die Form $f(x, y)$ in eine solche ihr äquivalente Form $A'x^2 + B'xy + C'y^2$ über, für die $(A', N) = 1$ ist. Es sei jetzt $a_1x^2 + b_1xy + c_1y^2$ die primitive Form, die die Zahl L darstellt. Es sei $A_1x^2 + B_1xy + C_1y^2$ die ihr äquivalente Form, für die $(A_1, L) = 1$ ist. Dann folgt also aus $L = A_1x_1^2 + B_1x_1y_1 + C_1y_1^2$, $D = B_1^2 - 4A_1C_1$, daß

$$\xi_1^2 - D \equiv 0 \pmod{L} \text{ mit } \xi_1 \equiv \frac{2A_1x_1 + B_1y_1}{y_1} \pmod{L}$$

lösbar ist. Wir können jetzt solche ganzen Zahlen x_0, y_0 des Körpers $K(\theta)$ finden, daß $L \mid f(x_0, y_0)$ ist. Denn ist $A_2x^2 + B_2xy + C_2y^2$ eine zu $ax^2 + bxy + cy^2$ äquivalente Form, für welche $(A_2, L) = 1$, so ist mit $2A_2t + B_2 \equiv \xi_1 \pmod{L}$

$$(2A_2t + B_2)^2 - D \equiv 0 \pmod{L}, \quad A_2t^2 + B_2t + C_2 \equiv 0 \pmod{L}.$$

Aus den Transformationsformeln erhalten wir somit die Werte von x_0 und y_0, wobei $(x_0, y_0) = 1$ ist. Die Zahlen ξ_2 und η_2, für welche gleichzeitig

$$\xi_2 \equiv x' \pmod{N}, \quad \eta_2 \equiv y' \pmod{N}, \quad \xi_2 \equiv x_0 \pmod{L}, \quad \eta_2 \equiv y_0 \pmod{L}$$

gilt, haben die Eigenschaft, daß für sie $(f(\xi_2, \eta_2), N) = 1$ und $L \mid f(\xi_2, \eta_2)$ ist. Es ist klar, daß man $(NL, \xi_2, \eta_2) = 1$, und da mit ξ_2 auch $\xi_2 + NLJ^h$ eine Lösung ist, wo

J sämtliche Primidealteiler von η_2 enthält, für die $(\xi_2, J) = 1$ ist, auch $(\xi_2, \eta_2) = 1$ annehmen kann. Somit existiert eine zu $f(x, y)$ äquivalente Form, für welche die Behauptung unseres Satzes gilt.

Satz 3. 1) *Aus jeder Form* $ax^2 + bxy + cy^2$ *der Determinante* $-Dq$, *wo* $(D, q) = 1$, q *eine ungerade Primzahl und* a, b, c *ganze rationale Zahlen sind, kann man mittels der Transformation*

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{-q}} \end{pmatrix},$$

wo $\alpha, \beta, \gamma, \delta$ *ganze rationale Zahlen sind und* $\alpha\delta - \beta\gamma = 1$ *ist, eine Form vom zweiten Typus erhalten.*

2) *Sind zwei Formen der Determinante* $-Dq$ *mit* $(D, q) = 1$ *und ganzen rationalen Koeffizienten, im rationalen Körper zueinander äquivalent, so sind die Formen vom zweiten Typus, die sich nach* 1) *ergeben, ebenfalls äquivalent.*

3) *Das Produkt zweier Formen vom ersten resp. vom zweiten Typus ist einer Form vom ersten resp. vom zweiten Typus im Körper* $K(\sqrt{-q})$ *äquivalent. Dabei erhält man das Produkt der Formen des zweiten Typus aus der Transformation*

$$\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{-q}} \end{pmatrix},$$

angewandt auf das Produkt der sich nach 1) *ergebenden Formen der Determinante* $-Dq$.

Beweis. 1) Nach Hilfssatz 3 kann man eine zu $ax^2 + bxy + cy^2$ im rationalen Körper äquivalente Form $Ax^2 + Bxy + Cy^2$ finden, für welche $q \mid C$ ist, Da $B^2 - 4AC = -Dq$ und q eine Primzahl ist, so muß zugleich $q \mid B$ sein, womit der Satz bewiesen ist.

2) Es seien die Formen

$$f(x, y) = ax^2 + bxy + cy^2, \quad f_1(x, y) = a_1x^2 + b_1xy + c_1y^2$$

der Determinante $-qD$ gegeben. Geht $f_1(x, y)$ mittels der Transformation $\begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix}$ in die Form $A_1x^2 + B_1\sqrt{-q}xy + C_1y^2$ über und ist $Ax^2 + B\sqrt{-q}xy + Cy^2$ die Form, aus der mittels der Transformation $\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-q} \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ die Form $f(x, y)$ sich ergibt $(\alpha\delta - \beta\gamma = \alpha_1\delta_1 - \beta_1\gamma_1 = 1)$, und sind $f(x, y)$, $f_1(x, y)$, der Transformation

$$\begin{pmatrix} u & v \\ w & t \end{pmatrix}, \quad ut - vw = 1$$

gemäß, im rationalen Körper äquivalent, so geht mittels der Transformation

$$\begin{pmatrix} G & \frac{H}{\sqrt{-q}} \\ P\sqrt{-q} & R \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-q} \end{pmatrix}\begin{pmatrix} G & H \\ P & R \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{-q}} \end{pmatrix}, \text{ wo } \begin{pmatrix} G & H \\ P & R \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} u & v \\ w & t \end{pmatrix}\begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix},$$

die Form $Ax^2 + B\sqrt{-q}xy + Cy^2$ in die Form $A_1x^2 + B_1\sqrt{-q}xy + C_1y^2$ über. Da

$$A\left(\frac{H}{\sqrt{-q}}\right)^2 + BHR + CR^2 = C_1, \quad (-qB^2 - 4AC, q) = (4AC, q) = 1,$$

so ist $(A, q) = 1$, und es muß $q \mid H$ sein. Sind also die Formen $f(x, y), f_1(x, y)$ im rationalen Körper eigentlich äquivalent, so sind die Formen vom zweiten Typus, welche den Formen $f(x, y)$, $f_1(x, y)$ gemäß 1) entsprechen, im Körper $K(\sqrt{-q})$ ebenfalls eigentlich äquivalent.

3) Sind die Formen vom ersten Typus, so ist der Satz klar. Es genügt nämlich, alle Operationen nur im rationalen Körper durchzuführen. Wir betrachten also nur den Fall des zweiten Typus genauer. Um das symbolische Produkt der Formen

$$\text{(I)}\ ax^2 + b\sqrt{-q}xy + cy^2, \qquad \text{(II)}\ a_1x^2 + b_1\sqrt{-q}xy + c_1y^2$$

zu finden, betrachten wir die der Form $a_1x^2 - qb_1xy - c_1qy^2$ äquivalente Form

$$Ax^2 + Bxy + Cy^2, \quad \text{wo} \quad (A, a) = 1 \quad \text{und} \quad q \mid A \quad \text{ist.}$$

Nach Hilfssatz 3 sind nämlich solche Zahlen A, B, C im rationalen Körper stets vorhanden. Wir können also $A = qA_1$, $B = qB_1$ setzen. Es seien jetzt m und m_1 ganze rationale Zahlen so, daß $2am - bq = 2Am_1 + B$ ist. Somit erhalten wir, daß in der Form $ax^2 + \beta xy + \gamma y^2$, die sich aus $ax^2 - bqxy - cqy^2$ mittels der Transformation $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ ergibt, und in der Form $qA_1x^2 + \beta_1xy + \gamma_1y^2$, in die die Form $qA_1x^2 + qB_1xy + Cy^2$ mittels der Transformation $\begin{pmatrix} 1 & m_1 \\ 0 & 1 \end{pmatrix}$ übergeht, $\beta = \beta_1$ ist. Es muß also

$$\beta^2 - 4a\gamma = \beta^2 - 4A\gamma_1, \quad a\gamma = A\gamma_1, \quad a \mid \gamma_1, \quad qA_1 \mid \gamma$$

sein (da $(A, a) = 1$ ist).

Demnach sind die Formen

$$ax^2 + \frac{\beta}{\sqrt{-q}}xy - \frac{\gamma}{q}y^2, \quad -A_1x^2 + \frac{\beta}{\sqrt{-q}}xy + \gamma_1y^2$$

komponierbar, und ihr Produkt ist ebenfalls eine Form vom zweiten Typus. Nach 2) sind die Formen (I) und $ax^2 + \frac{\beta}{\sqrt{-q}}xy - \frac{\gamma}{q}y^2$ äquivalent. Dasselbe gilt auch für die Formen (II) und $-A_1x^2 + \frac{\beta}{\sqrt{-q}}xy + \gamma_1y^2$. Es leuchtet ein, daß einerseits die Formen

$$-A_1x^2 + \frac{\beta}{\sqrt{-q}}xy + \gamma_1y^2, \qquad \gamma_1x^2 - \frac{\beta}{\sqrt{-q}}xy - A_1y^2,$$

andererseits die Formen

$$qA_1x^2 + \beta xy + \gamma_1y^2, \qquad \gamma_1x^2 - \beta xy + qA_1y^2$$

mittels der Transformation $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ineinander übergehen. Da $qA_1x^2 + \beta xy + \gamma_1y^2$ der Form $a_1x^2 - qb_1xy - c_1qy^2$ äquivalent ist, ist damit, wieder nach 2), der Satz bewiesen.

Hilfssatz 4. Sind zwei Formen vom zweiten Typus einer Form vom ersten Typus äquivalent, so sind die Formen der Determinante $-Dq$, aus denen man mittels der Transformation $\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{-q}} \end{pmatrix}$ *die Formen vom zweiten Typus erhält, einer Form*

$$f(x, y) = ax^2 + aq\varrho xy + cy^2$$

im rationalen Körper äquivalent, wo a, c ganze rationale Zahlen sind und $\varrho = 0$ oder 1 ist.

Beweis. Jede Form $a_1x^2 + b_1\sqrt{-q}xy + c_1y^2$ vom zweiten Typus, die einer Form $ax^2 + a\varrho xy + cy^2$, wo $\varrho = 0, 1$ und a, c ganze rationalen Zahlen sind, äquivalent ist, ist zugleich einer Form vom zweiten Typus $ax^2 + a\sqrt{-q}\varrho xy + cy^2$ äquivalent (vgl. den Anfang des Beweises von Satz 2). Es sei $Ax^2 - qBxy - Cqy^2$ eine Form, die nach Multiplikation mit $a_1x^2 - qb_1y - c_1qy^2$ im rationalen Körper die Form

$ax^2 - qa\varrho xy - cqy^2$ ergibt. Nach 3) von Satz 3 existiert eine solche Form, d. h. das symbolische Produkt

$$(a_1 x^2 + b_1 \sqrt{-q}\, xy + cy^2)\,(Ax^2 + B\sqrt{-q}\, xy + Cy^2)$$

ist der Form $ax^2 + a\sqrt{-q}\, xy + cy^2$ äquivalent. Es sei $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit $\alpha\delta - \beta\gamma = 1$ die Transformation, mittels der die Form

$$x^2 - D'y^2, \quad D' = \frac{D}{4}$$

in die Form $Ax^2 + B\sqrt{-q}\, xy + Cy^2$ übergeht. Dann ist $A = \alpha^2 - D'\gamma^2$. Ist eine der Zahlen α, γ nicht rational, so wird

$$A^2 = (\alpha\bar{\alpha} - D'\gamma\bar{\gamma})^2 + D'q\left(\frac{\alpha\bar{\gamma} - \gamma\bar{\alpha}}{\sqrt{-q}}\right)^2, \tag{12}$$

wo $\alpha\bar{\alpha} - D'\gamma\bar{\gamma}$, $\dfrac{\alpha\bar{\gamma} - \gamma\bar{\alpha}}{\sqrt{-q}}$ ganze rationale Zahlen sind. Nun kann als erster Koeffizient der Form $Ax^2 - Bqxy - Cqy^2$ jede beliebige durch diese Form eigentlich darstellbare Zahl angenommen werden. Ist nämlich $A_1x^2 + B_1xy + C_1y^2$, $(A_1, q) = 1$, eine beliebige äquivalente Form, so kann man eine Zahl m finden, für die $q \mid f(m, 1)$ ist (vgl. z. B. Hilfssatz 3). Die Transformation $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ wird also eine Form ergeben, die die entsprechende Eigenschaft hat. Demgemäß setzen wir für den ersten Koeffizienten der Form $Ax^2 + B\sqrt{-q}\, xy + Cy^2$, falls $q = 1$ oder q beliebig, aber $D' \equiv 1, 2 \pmod 4$ ist, den Wert $\dfrac{\mu}{(\mu, q)}$, wo μ die kleinste aller natürlichen durch die Form $Ax^2 - Bqxy - Cqy^2$ darstellbaren Zahlen bezeichnet. Ist aber $D' \equiv -1 \pmod 4$, so setzen wir für A in $Ax^2 + B\sqrt{-q}\, xy + Cy^2$ eine beliebige durch diese Form darstellbare rationale Primzahl p (nach einem bekannten analytischen Dirichlet-Schering-Weberschen Satze existieren stets unendlich viele solche Primzahlen; vgl. aber den nachfolgenden zweiten Beweis unseres Hilfssatzes 4). Nach der Gleichung (12) muß dann für $A = p$ die Form $Ax^2 - Bqxy - Cqy$ im rationalen Körper ambig sein. Dies ergibt sich unmittelbar aus der Tatsache, daß aus (12) entweder $p = D_1 u^2 + D_2 v^2$ oder $2p = D_1u^2 + D_2v^2$ folgt. Mit $2p$ ist aber auch p durch eine ambige Form darstellbar, denn $D_1D_2 = D$, und u, v sind ganze rationale Zahlen. Da p Primzahl ist, so sind alle Formen, durch die p darstellbar ist, eigentlich resp. uneigentlich äquivalent. Es sei also $A = \mu$, wo $(A, q) = 1$ ist. Es ist somit $\mu^2 \leqq \dfrac{Dq}{3}$, und aus (12) folgt für $2 \mid A$, $2 \mid \alpha\bar{\alpha} \pm D\gamma\bar{\gamma}$, also ist $\alpha\bar{\gamma} - \gamma\bar{\alpha} = 0$, denn

$$\left(\frac{\alpha\bar{\gamma} - \gamma\bar{\alpha}}{\sqrt{-q}}\right)^2 \leqq 1.$$

Für $q = 1$ ist $\alpha\bar{\gamma} - \gamma\bar{\alpha}$ gerade, also muß $\alpha\bar{\gamma} - \gamma\bar{\alpha} = 0$ sein. Ebenso muß $\alpha\bar{\gamma} - \gamma\bar{\alpha} = 0$ auch für $q \geqq 3$ gelten. Sonst wäre in der Gleichung (12) die rechte Seite $\equiv -1, 2 \pmod 4$ für $D' \equiv 1, 2 \pmod 4$, die linke dagegen $\equiv 1$ oder $0 \pmod 4$. Da $(\alpha, \gamma) = (\bar{\alpha}, \bar{\gamma}) = 1$ ist, so muß $\alpha = \varepsilon\bar{\alpha}$, $\gamma = \varepsilon\bar{\gamma}$ sein, wo ε eine gewisse Zahl ist, für die gleichzeitig

$$A = \alpha^2 - D'\gamma^2 = \varepsilon^2(\bar{\alpha}^2 - D'\bar{\gamma}^2) = \bar{\alpha}^2 - D'\bar{\gamma}^2, \quad \varepsilon^2 = 1, \ \varepsilon = \pm 1$$

ist. Die Zahlen α, γ sind also entweder ganz und rational oder gleichzeitig rein imaginär. Sind sie ganz und rational, so haben wir

$2\alpha\beta - 2D'\gamma\delta = B\sqrt{-q}$, $2\alpha\bar{\beta} - 2D'\gamma\bar{\delta} = -B\sqrt{-q}$, $\alpha(\beta + \bar{\beta}) = D'\gamma(\delta + \bar{\delta}) = 2D'\gamma g$, wo $2g = \delta + \bar{\delta}$. Da

$$\alpha\delta - \beta\gamma = 1, \quad -D'\gamma^2 = A - \alpha^2,$$

so ist

$$1 = \Re(\alpha\delta - \beta\gamma) = \alpha g - D'\frac{\gamma^2}{\alpha}g = \alpha g + \frac{A-\alpha^2}{\alpha}g = \frac{A}{\alpha}g \qquad (\Re x = \text{reeller Teil von } x).$$

Es ergibt sich somit aus

$$\alpha = Ag, \quad A^2g^2 - D'\gamma^2 = A, \quad (\alpha, \gamma) = (Ag, \gamma) = 1,$$

daß $A \mid D'$, d. h. die Form $Ax^2 - Bqxy - Cqy^2$ ambig ist. Sind aber die Zahlen α, γ rein imaginär (was wegen $\alpha\delta - \beta\gamma = 1$ nur für $q = 1$ möglich ist), so ergibt sich aus

$$2\alpha\beta - 2D'\gamma\delta = B\sqrt{-q}, \quad \alpha(\beta - \bar{\beta}) = D'\gamma(\delta - \bar{\delta}) = 2D'\gamma h,$$

wo $2h = \delta - \bar{\delta}$, daß

$$1 = \Re(\alpha\delta - \beta\gamma) = \alpha h - D'\frac{\gamma^2}{\alpha}h, \quad \alpha = h(\alpha^2 + A - \alpha^2) = hA$$

ist. Wegen

$$A = \alpha^2 = D'\gamma^2 = h^2A^2 - D'\gamma^2,$$

wo $(\alpha, \gamma) = (Ah, \gamma) = (A, \gamma) = 1$ ist, muß $A \mid D'$ sein. Daraus folgt, daß die Form $Ax^2 - Bqxy - Cqy^2$ auch in diesem Falle im rationalen Körper ambig ist. Demnach ist auch die Form $a_1x^2 - qb_1xy - c_1qy^2$ im rationalen Körper ambig. Da jede ambige Form einer Form $ax^2 + a\varrho xy + cy^2$ mit $\varrho = 0$ oder 1 äquivalent ist (s. Cahen S. 324 bis 327), ist Hilfssatz 4 bewiesen.

Zweiter Beweis (ohne Anwendung des analytischen Dirichlet-Schering-Weberschen Satzes) *des Hilfssatzes* 4.

Es sei wieder $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$, wo $\alpha\delta - \beta\gamma = 1$ ist, die Transformation, mittels der die Form $x^2 - \frac{D}{4}y^2$ in die Form $Ax^2 + B\sqrt{-q}xy + Cy^2$ übergeht. Dann ist

$$(13) \quad A = \alpha^2 - \frac{D}{4}\gamma^2, \quad C = \beta^2 - \frac{D}{4}\delta^2, \quad B\sqrt{-q} = 2\alpha\beta - 2\frac{D}{4}\gamma\delta.$$

Somit geht die Form $x^2 - \frac{D}{4}y^2$ mittels der Transformation $\begin{pmatrix}\bar{\alpha} & \bar{\beta}\\ \bar{\gamma} & \bar{\delta}\end{pmatrix}$ in die Form $Ax^2 - B\sqrt{-q}xy + Cy^2$ über, d. h.

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\bar{\delta} & -\bar{\beta}\\ -\bar{\gamma} & \bar{\alpha}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}\alpha\bar{\delta} + \beta\bar{\gamma} & \alpha\bar{\beta} + \beta\bar{\alpha}\\ \gamma\bar{\delta} + \delta\bar{\gamma} & \gamma\bar{\beta} + \delta\bar{\alpha}\end{pmatrix}$$

ist eine automorphe eigentliche Transformation der Form $x^2 - \frac{D}{4}y^2$.

Nach den Hilfssätzen 1 und 2 ist

$$\alpha\bar{\delta} + \beta\bar{\gamma} = \gamma\bar{\beta} + \delta\bar{\alpha}.$$

Daraus ergibt sich, daß die Zahl

$$r = \bar{\alpha}\delta - \beta\bar{\gamma} = \alpha\bar{\delta} - \bar{\beta}\gamma$$

eine ganze rationale Zahl ist. Aus den Gleichungen

$$\alpha\delta - \beta\gamma = 1, \quad \bar{\alpha}\delta - \beta\bar{\gamma} = r$$

erhält man

$$(14) \qquad \beta = \frac{-\bar{\alpha} + \alpha\gamma}{-\alpha\bar{\gamma} + \bar{\alpha}\gamma}, \qquad \delta = \frac{-\bar{\gamma} + \gamma r}{-\alpha\bar{\gamma} + \bar{\alpha}\gamma}.$$

Wie vorher bezeichnet der erste Koeffizient von $Ax^2 + B\sqrt{-q}xy + Cy^2$ den Quo-

tienten $\frac{\mu}{(\mu, q)}$, wo μ die kleinste aller natürlichen durch die Form $Ax^2 - Bqxy - Cqy^2$ darstellbaren Zahlen ist. Man erhält ihn aus

$$A^2 = \left(\alpha\bar{\alpha} - \frac{D}{4}\gamma\bar{\gamma}\right)^2 + \frac{Dq}{4}\left(\frac{\alpha\bar{\gamma} - \gamma\bar{\alpha}}{\sqrt{-q}}\right)^2 . \tag{15}$$

Wie wir im ersten Beweise gesehen haben, kann man $\alpha\bar{\gamma} - \gamma\bar{\alpha} \neq 0$ annehmen. Demnach ist, da $\mu \leqq \frac{Dq}{3}$,

$$\bar{\alpha}\gamma - \bar{\gamma}\alpha = \varepsilon\sqrt{-q}, \quad \varepsilon = \pm 1 ,$$

und nach den Gleichungen (14) ist

$$\varepsilon\delta\sqrt{-q} = -\bar{\gamma} + \gamma r, \quad \varepsilon\beta\sqrt{-q} = -\bar{\alpha} + \alpha r .$$

Setzen wir diese Werte in die Gleichung (13) für $B\sqrt{-q}$ ein, so ergibt sich

$$\varepsilon Bq = 2(\varepsilon\alpha\beta\sqrt{-q} - 2\frac{D}{4}\gamma\delta\varepsilon\sqrt{-q}) = 2[\alpha(-\bar{\alpha} + \alpha r) - \frac{D}{4}\gamma(-\bar{\gamma} + \gamma r)$$
$$= 2(\alpha^2 r - \frac{D}{4}\gamma^2 r - \alpha\bar{\alpha} + \frac{D}{4}\gamma\bar{\gamma})] .$$

Bezeichnen wir mit B_1 die Zahl $2(-\alpha\bar{\alpha} + \frac{D}{4}\gamma\bar{\gamma})$, so ist

$$B_1 = \varepsilon Bq - 2r\left(\alpha^2 - \frac{D}{4}\gamma^2\right) = \varepsilon Bq - 2rA .$$

Nach Gleichung (15) ist die Determinante der Form $Ax^2 + B_1xy + Ay^2$ gleich $-Dq$. Nun geht die Form $Ax^2 + \varepsilon Bqxy - Cy^2$ durch die Transformation $\begin{pmatrix} 1 & -r \\ 0 & 1 \end{pmatrix}$ in die Form $Ax^2 + B_1xy + Ay^2$ über. Da die Form $Ax^2 + B_1xy + Ay^2$ im rationalen Körper ambig ist (vgl. z. B. Cahen S. 327), so ist der Satz bewiesen.

Satz 4. *Die Anzahl der verschiedenen nichtäquivalenten Produkte $f\varphi$, wo f eine Form vom ersten, φ eine vom zweiten Typus ist, ergibt sich aus der Formel $\frac{hh'}{2^{v+\varrho}}$, wo h resp. h' die Klassenzahl der Formen der Determinante D resp. $-qD$ im rationalen Körper, v die Anzahl der verschiedenen ungeraden Primteiler der Zahl $D = 4D'$ bezeichnet und*

1) $\varrho = 0$ *ist für* $q \geqq 3$ *und* $D' \equiv 1 \pmod 4$,
2) $\varrho = 1$ *ist für* $q \geqq 3$ *und* $D' \equiv -1, 2 \pmod 4$,
3) $\varrho = 0$ *ist für* $q = 1$, *falls* $x^2 - D'y^2 = -1$ *nicht in ganzen rationalen Zahlen lösbar ist*,
4) $\varrho = -1$ *ist sonst* (*für* $q = 1$).

Beweis. Wir betrachten symbolische Produkte $f\Phi$, wo f resp. Φ eine binäre quadratische Form der Determinante D resp. $-qD$ mit ganzen rationalen Koeffizienten ist. Mit $f\varphi = |f\Phi|$, wo φ eine Form vom zweiten Typus ist, welche nach Satz 3, Fall 1) der Form Φ entspricht, werden wir den „Wert" von $f\Phi$ bezeichnen. Wir zählen jetzt alle möglichen Werte von $f\Phi$ ab. Es gilt nämlich, daß die Anzahl aller symbolischen Produkte $f\Phi$ gleich hh' ist. Ist jetzt $|f_1\Phi_1| = |f_2\Phi_2|$, so wird $f_1\varphi_1 = f_2\varphi_2$ sein, wo φ_1 resp. φ_2 die Form ist, die Φ_1 resp. Φ_2 nach Satz 3, Fall 1) entspricht. Werden im rationalen Körper die Formen f mit der Determinante D und Φ mit der Determinante $-qD$ durch die Gleichungen $f_1 f = f_2$, $\Phi_1\Phi = \Phi_2$ definiert, so gilt, wenn nur φ die Form vom zweiten Typus ist, die der Form Φ nach Satz 3, Fall 1) und 3) entspricht, daß $\varphi_1\varphi = \varphi_2$ und

$$|f\Phi| = f\varphi = \text{Einheitsform} \tag{16}$$

ist. Es sei zunächst $q \geqq 3$. Jeder Form φ, welche der Relation (16) genügt, entspricht eine und nur eine Form f. Denn sind dies f_1 und f_2, so wird f_1 der Form f_2 im Körper $K(\sqrt{-q})$ und mithin auch im rationalen Körper äquivalent sein. Nach Satz 2 ist die Form f einer Form der Determinante D äquivalent, die im rationalen Körper ambig ist. Ist v die Anzahl aller ungeraden Primteiler von D, so ist für $\frac{D}{4} = D' \equiv 1 \pmod 4$ die Zahl 2^v und für $D' \equiv -1, 2 \pmod 4$ die Zahl 2^{v+1} die Anzahl der ambigen Formen der Determinante D (s. z. B. Cahen S. 554—57). Da jeder ambigen Form Φ mit der Determinante $-Dq$, $q \geqq 3$, eine Form φ entspricht, die durch die Transformation $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ resp. $\begin{pmatrix} 1 & \frac{1-\sqrt{-q}}{2} \\ 0 & 1 \end{pmatrix}$ in eine ambige Form f vom ersten Typus übergeht, so finden sich genau 2^v resp. 2^{v+1} Formen Φ, für welche Formen f so existieren, daß (16) besteht. Demnach ist auch die Anzahl aller möglichen Paare f, Φ, für die (16) besteht, gleich 2^v, falls $D' \equiv 1 \pmod 4$ und gleich 2^{v+1}, falls $D' \equiv -1, 2 \pmod 4$ ist. Nun ist klar, daß die Anzahl aller möglichen Paare $f\Phi$, für welche $|f_k \Phi_k| = |f_g \Phi_g|$, ebenso groß ist. Somit ist die Anzahl sämtlicher Werte von $|f\Phi|$ gleich $\frac{hh'}{2^v}$ für $D' \equiv 1 \bmod 4$ und gleich $\frac{hh'}{2^{v+1}}$ für $D' \equiv -1, 2 \pmod 4$.

Es sei jetzt $q = 1$. Da die Zahl D' im Körper $K(i)$ quadratfrei ist, so muß D' ungerade sein. Ist $D' \equiv -1 \pmod 4$, so sind alle ambigen Formen der Determinante $-D$ Formen der Gestalt $ax^2 + cy^2$ äquivalent. Diese geht durch die Transformation $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ in die Form $ax^2 - cy^2$ über, die einer Form vom ersten Typus äquivalent ist. Nun muß auch für $D' \equiv 1 \pmod 4$ jede ambige Form der Determinante $-D$, welche nach der Transformation $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ einer Form vom ersten Typus äquivalent wird, einer Form der Gestalt $ax^2 + cy^2$ im rationalen Körper äquivalent sein. Es gilt nämlich, daß jede ambige Form entweder einer Form der Gestalt $ax^2 + cy^2$ oder der Gestalt $ax^2 + axy + cy^2$ äquivalent ist. Wir betrachten also nur den zweiten Fall. Da für $D' \equiv 1 \pmod 4$ jede ambige Form der Determinante D einer Form mit verschwindendem mittleren Koeffizienten äquivalent ist, so muß die Form $ax^2 - aixy - cy^2$ ebenfalls einer solchen Form äquivalent sein. Wir bezeichnen diese Form mit $dx^2 - ky^2$. Das symbolische Produkt $(ax^2 + axy + cy^2)(dx^2 + ky^2)$ ist im rationalen Körper einer ambigen Form äquivalent, welche die Gestalt $Ax^2 + Axy + Cy^2$ habe. Die Form $Ax^2 - Aixy - Cy^2$ muß aber im Körper $K(i)$ der Einheitsform äquivalent sein. Es sei $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ die Transformation, welche die Einheitsform $x^2 - D'y^2$ in die Form $Ax^2 - Aixy - Cy^2$ überführt. Dann ist also

$$\alpha^2 - D'\beta^2 = \bar{\alpha}^2 - D'\bar{\beta}^2 = A, \quad R^2 + D'S^2 = A^2, \quad R = \alpha\bar{\alpha} - D'\beta\bar{\beta}, \quad Si = \alpha\bar{\beta} - \beta\bar{\alpha}.$$

Die Zahlen R und S sind ganz und rational. Da $D' \equiv 1 \pmod 4$ und die Zahl A gerade ist, so müssen beide Zahlen R, S gerade sein. Ferner ist $\frac{A}{2} \Big| \frac{D}{4}$, und daher muß, da D' quadratfrei ist, $A \mid R$ und $A \mid S$ sein. Dies ist nur möglich für $\alpha\bar{\beta} - \beta\bar{\alpha} = Si = 0$. Es müssen also die Zahlen α, β entweder gleichzeitig rational oder gleichzeitig rein imaginär

sein. Der zweite Fall ist aber unmöglich. Denn wäre $\alpha = \alpha_1 i$, $\beta = \beta_1 i$, wo α_1, β_1 ganze rationale Zahlen sind, so würde sich aus $2 \mid A$

$$A = -\alpha_1^2 + D'\beta_1^2 \equiv -1 + 1 \equiv 0 \pmod 4$$

ergeben. Aus $-A^2 + 4Ac = D$ folgt aber $(A, 4) \leqq 2$. Ebenso können nicht die Zahlen α, β ganz und rational sein, denn aus $2 \mid A$ folgt wieder $A = \alpha^2 - D'\beta^2 \equiv 0 \pmod 4$. Die Anzahl der Formen Φ, für welche (16) besteht, beträgt also 2^{v-1} (Cahen S. 555—56). Ist die Gleichung $x^2 - D'y^2 = -1$ lösbar, so sind zwei Formen der Gestalt

$$a_1x^2 + b_1xy + c_1y^2, \qquad -a_1x^2 + b_1xy - c_1y^2$$

der Determinante D im rationalen Körper zueinander eigentlich äquivalent. Es ist dann nämlich die Form $x^2 - D'y^2$ der Form $-x^2 + D'y^2$ und demnach auch der Form $-x^2 + b_1xy - a_1c_1y^2$ äquivalent. Multiplizieren wir die Formen $a_1x^2 + b_1xy + c_1y^2$ und $-x^2 + b_1xy - a_1c_1y^2$ miteinander, so erhalten wir die Form $-a_1x^2 + b_1xy - c_1y^2$. Nach Satz 1 ist also in diesem Falle auch im Körper $K(i)$ eine Form vom ersten Typus einer zweiten Form desselben Typus dann und nur dann äquivalent, wenn sie im rationalen Körper äquivalent sind. Demnach beträgt die Anzahl der Paare, für welche (16) besteht, 2^{v-1}, woraus folgt, daß die Anzahl aller verschiedenene Werte von $|f\Phi|$ gleich $\dfrac{hh'}{2^{v-1}}$ ist.

Es sei jetzt die Gleichung $x^2 - D'y^2 = -1$ in ganzen rationalen Zahlen unlösbar. Zwei beliebige Formen $a_1x^2 + b_1xy + c_1y^2$, $-a_1x^2 + b_1xy - c_1y^2$ können dann nicht zueinander äquivalent sein. Wir haben nämlich auf Grund der Kompositionstheorie:

$$\begin{aligned}(a_1x^2 + b_1xy + c_1y^2)(-a_1x^2 - b_1xy - c_1y^2) &= (a_1x^2 + b_1xy + c_1y^2)(-c_1x^2 + b_1xy - a_1y^2)\\ &= (-a_1c_1x^2 + b_1xy - y^2).\end{aligned}$$

Es entsprechen also jeder Form Φ zwei im rationalen Körper nicht äquivalente Formen f, für welche (16) gilt. Demnach beträgt die Anzahl aller Paare f, Φ, für welche (16) gilt, 2^v, und die Anzahl der verschiedenen Werte von $|f\Phi|$ ist gleich $\dfrac{hh'}{2^v}$.

Unser Ziel ist jetzt, notwendige und hinreichende Bedingungen dafür anzugeben, wann eine Form der Determinante D im Körper $K(\sqrt{-q})$ durch ein Produkt von Formen vom ersten und zweiten Typus darstellbar ist.

Definition 2. Ist $\alpha x^2 + \beta xy + \gamma y^2$ eine primitive quadratische Form mit Koeffizienten, die ganze Zahlen des Körpers $K(\sqrt{-q})$ sind, so werden wir die Charaktere

$$\left(\frac{\bar{v}, D'}{\mathfrak{d}_1}\right), \ldots, \left(\frac{\bar{v}, D'}{\mathfrak{d}_s}\right), \quad D' = \frac{D}{4}, \quad \mathfrak{d}_s \mid \mathfrak{d}, \qquad s = 1, 2, \ldots, r,$$

die zum Ideal $\left[\alpha, \dfrac{\beta + \sqrt{D}}{2}\right]$ gehören, auch als zur Form $\alpha x^2 + \beta xy + \gamma y^2$ gehörige Charaktere bezeichnen (vgl. Hilbert § 17).

Anmerkung. Jeder Charakter $\left(\dfrac{\bar{v}, D'}{\mathfrak{d}}\right)$ ist bekanntlich Normenrestsymbol. Es ist $\bar{v} = \varepsilon\alpha$, wo ε eine Einheit des Grundkörpers $K(\sqrt{-q})$ ist. Wenn es in $K(\sqrt{-q})$ eine und nur eine Einheit ξ gibt, für die nicht alle Normenrestsymbole $\left(\dfrac{\xi, D'}{\mathfrak{d}_s}\right) = 1$ sind, so ist $r = t - 1$, wo t die Anzahl der verschiedenen Primidealteiler von $\mathfrak{d}$ bedeutet. Ferner haben, da allen Idealen einer Klasse dasselbe Charakterensystem entspricht, äquivalente Formen ebenfalls dasselbe Charakterensystem (vgl. Hilbert § 17).

Definition 3. Alle Formen, denen ein und dasselbe Charakterensystem entspricht, bilden ein Geschlecht. Sind alle Charaktere eines Geschlechtes gleich 1, so bezeichnen wir dieses Geschlecht als Hauptgeschlecht.

Satz 5. *Ist* $ax^2 + bxy + cy^2$ *eine zum Hauptgeschlecht gehörige Form der rationalzahligen Determinante* D *und gehören die Koeffizienten einem imaginär-quadratischen Körper* $K(\sqrt{-q})$ *mit ungerader Klassenzahl an,* $q \neq 2$, *so ist die Gleichung*

$$ax^2 + bxy + cy^2 = \varepsilon z^2, \quad \varepsilon = \pm 1 \text{ bzw. } \varepsilon = \pm i \text{ für } q = 1$$

(*wo ein Charakter sich reduziert*) *in ganzen Zahlen des Körpers* $K(\sqrt{-q})$ *lösbar, wobei* $(z, D) = 1$ *angenommen werden kann.*

Beweis. Zunächst bemerken wir, daß man nach Hilfssatz 3 $(a, D) = 1$ annehmen kann. Denn ist der Satz für eine beliebige zu $ax^2 + bxy + cy^2$ äquivalente Form bewiesen, so gilt er auch für die gegebene Form. Wir wollen jetzt beweisen, daß die Gleichung

$$ax^2 + bxy + cy^2 = \varepsilon z^2, \tag{17}$$

wo ε Einheit des Körpers $K(\sqrt{-q})$ ist, in ganzen Zahlen des Körpers $K(\sqrt{-q})$ lösbar ist. Multiplizieren wir beide Seiten dieser Gleichung mit a, so erhalten wir

$$X^2 - D'y^2 = \varepsilon a z^2, \quad X = ax + \frac{b}{2}y, \quad D' = \frac{D}{4}. \tag{18}$$

Bezeichnet t die Anzahl sämtlicher Primteiler der Relativdiskriminante $\mathfrak{d}$, so ist die Anzahl der Charaktere gleich $t - 1$ oder t, je nachdem, ob für mindestens einen Teiler $\mathfrak{d}_s$ von $\mathfrak{d}$ das Symbol $\left(\frac{\varepsilon, D'}{\mathfrak{d}_s}\right) = -1$ ist oder nicht. Es gilt nämlich, daß ± 1 die einzigen Einheiten ε des Körpers $K(\sqrt{-q})$ für $q > 3$ sind. Für $q = 1$ sind es $\varepsilon = \pm 1, \pm i$, für $q = 3$ dagegen $\varepsilon = \pm 1, \pm \omega = \pm \bar{\omega}^2, \pm \bar{\omega} = \pm \omega^2$, wo $\omega = \frac{-1 + \sqrt{-3}}{2}$ ist. Es sei jetzt $\bar{v}$ die Zahl, durch die die Charaktere der Form $ax^2 + bxy + cy^2$ definiert sind. Da $\bar{v}$ mit a assoziiert ist (vgl. Hilbert § 17), so gilt für $q \geqq 3$ die Gleichung $\bar{v} = \pm a$. Für $q = 3$ ist $\bar{v} = \pm \varepsilon a$, wo $\varepsilon = \pm 1, \frac{-1 + \sqrt{-3}}{2}$, und für $q = 1$ ist $\bar{v} = \pm a, \pm ia$. Da $ax^2 + bxy + cy^2$ zum Hauptgeschlecht gehört, so ist nach Definition der Zahl $\bar{v}$ für jeden Primteiler $\mathfrak{d}_s$ der Relativdiskriminante $\mathfrak{d}$ das Symbol $\left(\frac{\bar{v}, D'}{\mathfrak{d}_s}\right) = 1$. Ist $(\mathfrak{d}, 2) = 1$, so wird für sämtliche zu 2 primen Primideale (vgl. Hilbert § 25):

$$\prod_{(\mathfrak{w})} \left(\frac{\bar{v}, D'}{\mathfrak{w}}\right) = 1.$$

Mit $(\mathfrak{d}, 2) = 1$ ist auch D' ungerade, folglich ist (vgl. Hilbert § 39)

$$\prod_{(\mathfrak{w})} \left(\frac{\bar{v}, D'}{\mathfrak{w}}\right) = 1,$$

wo das Produkt über sämtliche Primideale $\mathfrak{w}$ des Körpers $K(\sqrt{-q})$ erstreckt werden soll. Für $(\mathfrak{d}, 2) = 1$ erhält man aus diesen Relationen und aus der Definition des Normenrestsymbols für quadratfreie $\bar{v}$ (s. Hilbert § 11), da die Zahl 2 in $K(\sqrt{-q})$, $1 \leqq q \neq 2$, entweder unzerlegbar oder gleich $i(1 - i)^2$ ist:

$$\left(\frac{\bar{v}, D'}{1 - i}\right) = 1, \quad \left(\frac{\bar{v}, D'}{2}\right) = 1 \tag{19}$$

und für jeden Primteiler $\mathfrak{p}$ der Zahl $\bar{v}$ (vgl. wieder Hilbert § 11):

$$\left(\frac{\bar{v}, D'}{\mathfrak{p}}\right) = \left(\frac{D'}{\mathfrak{p}}\right), \tag{20}$$

also $= 1$. Für $(\mathfrak{d}, 2) \neq 1$ erhält man die zweite Gleichung (19) unmittelbar aus der Definition der Zahl $\bar{v}$ und des Hauptgeschlechtes. Analog gelten auch die Relationen (20). Ist also $\mathfrak{p}$ ein Primideal, das weder in $\bar{v}$ noch in D aufgeht, so ist (s. Hilbert, Satz 10) $\left(\frac{\bar{v}, D'}{\mathfrak{p}}\right) = 1$. Alles zusammen ergibt, daß für jedes Primideal $\mathfrak{w}$ die Relation $\left(\frac{\bar{v}, D'}{\mathfrak{p}}\right) = 1$ gilt. Somit erhält man, wieder nach einem Hilbertschen Satze (s. Hilbert § 43 und 44), daß die Gleichung (18) für ganze Zahlen des Körpers $K(\sqrt{-q})$ lösbar ist. Da $(a, D) = 1$ ist, so muß auch $(b, a) = 1$ sein, und demnach ist die Gleichung $X = at + \frac{b}{2}y$ für ganze Zahlen des Körpers $K(\sqrt{-q})$ lösbar. Setzen wir dies in die Gleichung (18) ein, so erhalten wir, daß die Gleichung (17) für ganze Zahlen des Körpers $K(\sqrt{-q})$ lösbar ist. Nun ergibt sich (da die Einheiten im Körper $K(\sqrt{-q})$ für $q > 3$ gleich ± 1 sind, für $q = 3$ aber $\varepsilon = \pm\omega = \pm\bar{\omega}^2$ oder $\varepsilon = \pm\bar{\omega} = \pm\omega^2$ mit $\omega = \frac{-1+\sqrt{-3}}{2}$, daß die Gleichung (17) für $\varepsilon = \pm 1, \pm i$, in ganzen Zahlen des Körpers $K(\sqrt{-q})$ lösbar ist. Ist x_0, y_0, z_0 ein Lösungssystem dieser Gleichung, so erhalten wir, daß durch die Transformation $\begin{pmatrix} x_0 & p \\ y_0 & q \end{pmatrix}$ mit $x_0 q - y_0 p = 1$ die Form $f(x, y) = \bar{\varepsilon}ax^2 + \bar{\varepsilon}bxy + \bar{\varepsilon}cy^2$, wo $\varepsilon\bar{\varepsilon} = 1$ ist, in die Form

$$z_0^2 x^2 + Bxy + f(p, q)y^2, \qquad B = 2\varepsilon a x_0 p + b^2\varepsilon(x_0 q + p y_0) + 2\varepsilon c y_0 q$$

übergeht. Diese ist aber ihrerseits dem symbolischen Quadrate der Form

$$z_0 x^2 + Bxy + z_0 f(p, q)y^2$$

äquivalent. Daraus ergibt sich, daß $f(x, y)$ Quadratzahlen darstellt, die nach Hilfssatz 3 in bezug auf eine beliebige Zahl relativ prim sind.

Definition 4. Eine binäre quadratische Form werden wir rationalfähig nennen, wenn sie ganze rationale Zahlen darstellt; für $q = 1$ soll sie auch dann rationalfähig genannt werden, wenn sie rein imaginäre Zahlen darstellt.

Satz 6. *Die notwendige und hinreichende Bedingung dafür, daß eine binäre quadratische Form $f(x, y)$ rationalfähig ist, lautet:*

1) *die Form ist ein Produkt einer Form vom ersten und einer vom zweiten Typus oder*

2) *ihre Charaktere erfüllen die Relationen*

$$(21)\quad \left(\frac{\bar{v}, D'}{\alpha_1}\right)\left(\frac{\bar{v}, D'}{\bar{\alpha}_1}\right) = 1, \ldots, \left(\frac{\bar{v}, D'}{\alpha_g}\right)\left(\frac{\bar{v}, D'}{\bar{\alpha}_g}\right) = 1; \qquad \left(\frac{\bar{v}, D'}{Q_1}\right) = 1, \ldots \left(\frac{\bar{v}, D'}{Q_l}\right) = 1,$$

wo $P_k = \alpha_k\bar{\alpha}_k$ die zerlegbaren ungeraden und Q_m die unzerlegbaren ungeraden rationalen Primteiler von D bezeichnen.

Beweis. Es sei $\varphi(x, y) = Ax^2 + Bxy + Cy^2$ eine binäre quadratische Form vom ersten resp. zweiten Typus der Determinante D, für welche die Gaußschen Charaktere die Relationen

$$\left(\frac{\bar{v}, D'}{\alpha_k}\right) = \left(\frac{A}{P_k}\right), \quad \left(\frac{\bar{v}, D}{Q_m}\right) = \left(\frac{A}{Q_m}\right) \quad (k = 1, 2, \ldots, g;\ m = 1, 2, \ldots, s)$$

erfüllen. Da für $q \geqq 3$ der Determinante $-qD$ im rationalen Körper mehr Charaktere entsprechen als der Deteminante D, und für $q = 1$ einer der Determinanten $D, -D$ mehr Charaktere entsprechen als der zweiten, so ist eine solche Form $\varphi(x, y)$ stets vorhanden. Nun ist jede ganze rationale Zahl gleichzeitig quadratischer Rest resp. Nichtrest in bezug auf α_k und $\bar{\alpha}_k$. Andererseits ist A quadratischer Rest jeder Zahl Q_m

im Körper $K(\sqrt{-q})$. Das symbolische Produkt

$$F(x, y) = f(x, y)\varphi(x, y) = kx^2 + lxy + my^2$$

gehört also, sofern für $f(x, y)$ die Relationen (21) bestehen, zum Hauptgeschlecht. Nach Hilfssatz 4 ist demnach die Gleichung

$$kx^2 + lxy + my^2 = \varepsilon z^2, \quad \varepsilon = \pm 1, \quad \varepsilon = \pm i$$

in ganzen Zahlen des Körpers $K(\sqrt{-q})$ lösbar und dabei $(z, D) = 1$. Offenbar können wir annehmen, daß die Zahlen x, y, z keinen gemeinschaftlichen ganzen Teiler haben. Ist jetzt π ein beliebiger Primidealteiler der Zahl z, so sind die Kongruenzen

$$(22) \qquad \xi^2 - D \equiv 0 \pmod{\pi}, \quad \xi^2 - D \equiv 0 \pmod{\bar{\pi}}$$

lösbar. Es sind also auch, da $(\pi, 2D) = 1$ ist, die Kongruenzen

$$\xi^2 - D \equiv 0 \pmod{N(\pi)}, \qquad \xi^2 - D \equiv 0 \pmod{N(\pi)^n},$$

mit natürlichem n, lösbar. Ferner folgt aus der Gleichung

$$(\xi^2 - D)(\bar{\xi}^2 - D) = (\xi\bar{\xi} \mp D)^2 - D(\xi \mp \bar{\xi})^2,$$

daß entweder $(\xi + \bar{\xi}, N(\pi))$ oder $(\xi - \bar{\xi}, N(\pi)) = 1$ ist. Ist nämlich $(\xi + \bar{\xi}, N(\pi)) \neq 1$, so muß $N(\pi) \mid (\xi + \bar{\xi})$ sein. Und wenn $(\xi - \bar{\xi}, N(\pi)) \neq 1$ ist, folgt, daß $(2\xi, N(\pi)) \neq 1$ ist, was $(\pi, D) \neq 1$ ergibt, und dies steht im Widerspruch zu $(z, 2D) = 1$. Die Zahl $N(\pi)^n$ ist also im rationalen Körper entweder durch eine Form vom ersten resp. vom zweiten Typus eigentlich darstellbar. Sind die Zahlen π und $\bar{\pi}$ assoziiert (d. h. $\pi^2 = N(\pi)$), so kann π^n höchstens zweimal durch eine Form der Determinante D darstellbar sein. Ist nämlich $A_1x_0^2 + B_1x_0y_0 + C_1y_0^2$ eine, so ist $A_1x_0 - B_1x_0y_0 + C_1y_0$ die zweite Darstellung. Es sei also $N(\pi)$ eine rationale Primzahl. Dann bilden die natürlichen Zahlen

$$1, 2, \ldots, N(\pi)^k,$$

wo k eine beliebige natürliche Zahl ist, im Körper $K(\sqrt{-q})$ ein Restsystem (mod π_k). Da mit der Kongruenz (22) auch die Kongruenz

$$\xi^2 - D \equiv 0 \pmod{\pi^k}$$

im Integritätsbereich der ganzen algebraischen Zahlen von $K(\sqrt{-q})$ lösbar ist, so kann man ξ als eine ganze rationale Zahl b annehmen. Nun sind die binären quadratischen Formen der Determinante D, welche die Zahl π^k darstellen, einer der Formen $\pi^kx^2 + \varepsilon bxy + \bar{\pi}^kcy^2$, $\varepsilon = \pm 1$, $b^2 - 4(\pi\bar{\pi})^kc = D$ eigentlich äquivalent. Wir betrachten jetzt die Gleichung

$$(23) \quad \left(\pi^k x + \frac{b + \sqrt{D}}{2} y\right)^2$$

$$= \frac{\left(\pi^k x + \frac{b + \sqrt{D}}{2} y\right)\left(\bar{\pi}^k x_1 + \frac{b + \sqrt{D}}{2} y_1\right)\left(\pi^k x + \frac{b + \sqrt{D}}{2} y\right)\left(\bar{\pi}^k x_2 + \frac{-b + \sqrt{D}}{2} y_2\right)}{\left(\bar{\pi}^k x_1 + \frac{b + \sqrt{D}}{2} y_1\right)\left(\bar{\pi}^k x_2 + \frac{-b + \sqrt{D}}{2} y_2\right)}.$$

Da der Nenner die Einheitsform ergibt, so folgt, daß das symbolische Produkt

$$(\pi^kx^2 + bxy + \bar{\pi}^kcy^2)^2 = \pi^{2k}x^2 + bxy + \bar{\pi}^k\frac{c}{\pi^k}y^2$$

dem Produkte

$$\left(\pi^k\bar{\pi}^kX^2 + bXY + \frac{b^2 - D}{4\pi^k\bar{\pi}^k}Y^2\right)\left(\pi^k\bar{\pi}^kX_1^2 + BX_1Y_1 + \frac{B^2 - D}{4\pi^k\bar{\pi}^k}\right)$$

gleich ist, wobei man die rein imaginäre Zahl B folgendermaßen bestimmen kann: Da π und $\bar{\pi}$ nicht assoziiert sind, so ist die Kongruenz

$$z^2 + q \equiv 0 \qquad (\mathrm{mod}\ N(\pi))$$

und mithin auch die Kongruenz

$$z^2 + q \equiv 0 \qquad (\mathrm{mod}\ N(\pi^k))$$

in ganzen rationalen z lösbar. Somit ist die Kongruenz

$$b^2 + qB_1^2 \equiv 0 \qquad (\mathrm{mod}\ N(\pi^k))$$

mit ganzen rationalen B_1 lösbar. Daraus ergibt sich z. B.

$$b + \sqrt{-q}\, B_1 \equiv 0 \qquad (\mathrm{mod}\ \pi^k),$$
$$b - \sqrt{-q}\, B_1 \equiv 0 \qquad (\mathrm{mod}\ \bar{\pi}^k).$$

Setzen wir $b + \sqrt{-q}\, B_1 = h\pi^k$, so wird

$$b - \sqrt{-q}\, B_1 = \bar{h}\bar{\pi}^k, \qquad \sqrt{-q}\, B_1 = -b + h\pi^k = b - \bar{h}\bar{\pi}^k;$$
$$\sqrt{-q}\, B_1 \equiv -b\ (\mathrm{mod}\ \pi^k), \qquad \sqrt{-q}\, B_1 \equiv b\ (\mathrm{mod}\ \bar{\pi}^k)$$

und somit kann man $B = -\sqrt{-q}\, B_1$ setzen. Demnach erhält man aus der Gleichung (23), daß die Form $\pi^{2k}x^2 + bxy + \bar{\pi}^{2k}cy^2$ als Produkt von Formen des ersten und zweiten Typus angenommen werden kann, und somit ist auch die Form $kx^2 + lxy + my^2$ Produkt von Formen des ersten und zweiten Typus. Da im Integritätsbereich der ganzen Zahlen von $K(\sqrt{-q})$ jede rationale Zahl quadratischer Rest in Bezug auf Q_l resp. gleichzeitig quadratischer Rest oder Nichtrest in Bezug auf die konjugiert imaginären Faktoren α_k und $\bar{\alpha}_k$ ist, so ist der Satz bewiesen.

Damit ergibt sich der Beweis für unseren

Hauptsatz. *Es sei $K(\sqrt{-q})$, $q \neq 2$, ein imaginär-quadratischer Körper mit ungerader Klassenzahl, $D > 2$ eine natürliche Zahl, die für $q = 1$ größer als 12 und für die $D' = \frac{D}{4}$ eine ganze durch keine Quadratzahl des Körpers $K(\sqrt{-q})$ teilbare Zahl ist; ferner sei h die Klassenzahl der binären quadratischen Formen der Determinante D im rationalen Körper, h_1 die Klassenzahl der binären quadratischen Formen der Determinante $-qD$ ebenfalls im rationalen Körper. Dann gilt:*

Die Klassenzahl H der binären quadratischen Formen der Determinante D, deren Koeffizienten ganze Zahlen des Körpers $K(\sqrt{-q})$ sind, wird für $q \geqq 3$ durch $H = \frac{hh'}{2}$ gegeben. Ist $q = 1$, so ist $H = hh'$ oder $2hh'$, je nachdem $x^2 - D'y^2 = -1$ in ganzen rationalen Zahlen lösbar ist oder nicht

Beweis. Nach Satz 4 und 5 ist die Anzahl aller rationalfähigen Formen $\frac{hh'}{2^{v+\varrho}}$, wo v und ϱ wie in Satz 4 definiert sind. Beträgt die Anzahl der zur Determinante D gehörigen Charaktere r, so ist die Anzahl der Geschlechter 2^{r-1} und die Anzahl der Geschlechter, denen rationalfähige Formen angehören, 2^{g+j}, wo g die Anzahl der zerlegbaren ungeraden rationalen Primteiler der Relativdiskriminante $\mathfrak{d}$ bezeichnet und $j = -1$ oder $= 0$ ist, je nachdem ein Charakter unterdrückt war oder nicht (s. Definition 2 dieses Teiles und vgl. Hilbert § 17). Es gilt nämlich, daß sich ein Charakter (resp. Normenrestsymbol) nur unter folgenden Bedingungen reduziert (s. Anmerkung zur Definition 2): Im Falle $q > 3$ nur dann, wenn (die Relation $N(\mathfrak{d}_k) \equiv 3\ (\mathrm{mod}\ 4)$ besteht, d. h.) $N(\mathfrak{d}_k)$ eine rationale

Primzahl ist. Denn im Körper $K(\sqrt{-q})$ ist für $q > 3$ jede Einheit gleich ± 1 und $\left(\frac{-1, D}{\mathfrak{d}_k}\right) = \left(\frac{-1}{\mathfrak{d}_k}\right) = -1$ (also muß $N(\mathfrak{d}_k) \equiv 3 \pmod 4$ sein). Im Falle $q = 3$ folgt (da $\pm\omega = \pm\bar{\omega}^2$, $\pm\bar{\omega} = \pm\omega^2$ ist) aus $\left(\frac{\varepsilon, D'}{\mathfrak{d}_k}\right) = -1$, daß ebenfalls $\left(\frac{-1, D'}{\mathfrak{d}_k}\right) = -1$, also wieder $N(\mathfrak{d}_k) \equiv 3 \pmod 4$ sein muß, d. h. $N(\mathfrak{d}_k)$ kein rationales Quadrat sein kann. Ferner ergibt sich im Körper $K(i)$ aus $\left(\frac{\varepsilon, D'}{\mathfrak{d}_k}\right) = -1$, da hier $\left(\frac{-1, D'}{\mathfrak{d}_k}\right) = 1$ ist, daß $\left(\frac{i, D'}{\mathfrak{d}_k}\right) = -1$ sein muß, d. h. $N(\mathfrak{d}_k)$ wieder kein rationales Quadrat ist.

Es ergibt sich also $r = g + j + v + \varrho$ für $q \geqq 3$. Da in jedem Geschlechte

$$\frac{hh'}{2^{g+j}\,2^{v+\varrho}}$$

Formen vorkommen, so beträgt die Anzahl H aller Formen

$$H = 2^{r-1}\,\frac{hh'}{2^{g+j}\,2^{v+\varrho}} = \frac{hh'}{2}\,.$$

In $K(i)$ ist mit $Ax^2 + Bxy + Cy^2$ auch die zur selben Hyperklasse gehörige Form (s. S. 181) $f_1(x, y) = iAx^2 + Bxy - Ciy^2$ rationalfähig. Nun sind diese Formen nicht äquivalent. Sonst wäre die Gleichung $i = x^2 - \frac{D}{4}y^2$ resp. die Gleichung $-i = \bar{x}^2 - \frac{D}{4}\bar{y}^2$ im Körper $K(i)$ lösbar, was wegen

$$1 = \left(x\bar{x} - \frac{D}{4}\,y\bar{y}\right)^2 - \frac{D}{4}\,(x\bar{y} - y\bar{x})^2$$

unmöglich ist. Wäre nämlich $x\bar{y} - y\bar{x} = 0$, so wäre $x = \varepsilon\bar{x}$, $y = \varepsilon\bar{y}$, $\varepsilon \mid 1$, was wegen $(x, y) = 1$ ergibt, daß $x^2 - \frac{D}{4}y^2$ eine ganze rationale Zahl ist. Da $f\varphi$ ungerade Zahlen darstellt, wo f eine Form vom ersten und φ vom zweiten Typus ist, so ist $ix^2 - D'y^2$ und mithin $f_1(x, y)$ einer solchen Form nicht äquivalent. Demnach ist $R = 2r$, wo R bzw. r die Anzahl der nicht äquivalenten rationalfähigen Klassen bzw. Hyperklassen ist.

Anmerkung 1. Es ist hier von Wichtigkeit zu betonen, daß die Tatsache, daß die Gleichung $ax^2 + bxy + cy^2 = \varepsilon z^2$, $\varepsilon = \pm 1$, $\varepsilon = \pm i$ in ganzen algebraischen Zahlen lösbar ist (s. Satz 5), für den Beweis des Hauptsatzes von wesentlicher Bedeutung ist. Nur dann können wir in der Gleichung (23) annehmen, daß b eine ganze rationale Zahl ist.

Anmerkung 2. Ebenso ist die Voraussetzung, daß die Klassenzahl von $K(\sqrt{-q})$ ungerade ist, von wesentlicher Bedeutung. Es sind nämlich nur für solche Körper die Hilbertschen Ergebnisse bewiesen.

Eingegangen 15. Juni 1935.

Zur Reinhardtschen Kennzeichnung der Kreisbogen.

Aus einem Schreiben an Herrn Reinhardt.

Von *Otto Haupt* in Erlangen.

---

1. Die von Ihnen vermutete Kennzeichnung der Kreisbogen [1]), auf welche Sie mich neulich aufmerksam machten, kann folgendermaßen ausgesprochen werden. Wir definieren: Eine Punktmenge $\mathfrak{M}$ möge *lokal in sich kongruent* heißen, wenn zu *irgend* zwei Punkten P_1, P_2 von $\mathfrak{M}$ stets Umgebungen $\mathfrak{U}(P_1;\mathfrak{M})$ und $\mathfrak{U}(P_2;\mathfrak{M})$ auf $\mathfrak{M}$ sich finden lassen von folgender Art: $\mathfrak{U}(P_1;\mathfrak{M})$ und $\mathfrak{U}(P_2;\mathfrak{M})$ sind durch kongruente Abbildung ineinander überführbar, wobei P_1 auf P_2 abgebildet wird [1a]). Dabei ist z. B. $\mathfrak{U}(P_1;\mathfrak{M})$ der Durchschnitt von $\mathfrak{M}$ mit einer (zweidimensionalen) Umgebung $\mathfrak{U}(P_1)$ von P_1 in der Ebene, also: $\mathfrak{U}(P_1;\mathfrak{M}) = \mathfrak{M} \frown \mathfrak{U}(P_1)$. Dann lautet die fragliche Behauptung:

Jeder ebene, lokal in sich kongruente Jordanbogen $\mathfrak{B}$ *ist ein Kreisbogen oder eine Strecke* [2]).

Sie selbst haben (vgl. Fußnote 1, a. a. O.) den Beweis dieser Behauptung bereits erbracht: Erstens für den Fall eines Jordanbogens $\mathfrak{B}$ mit stückweise stetiger Krümmung; zweitens für den Fall, daß die „Kongruenzumgebungen" $\mathfrak{U}(P_1;\mathfrak{B}) = \mathfrak{B} \frown \mathfrak{U}(P_1)$ für alle P_1 von $\mathfrak{B}$ eine „von Null verschiedene untere Grenze" besitzen, d. h. daß die zu den $\mathfrak{U}(P_1;\mathfrak{B})$ gehörigen $\mathfrak{U}(P_1)$ sämtlich eine feste Kreisscheibe enthalten. Nachstehend soll nun die Behauptung auch ohne einschränkende Annahmen über den Jordanbogen bewiesen werden.

2. Zum *Beweise* unserer Behauptung bemerken wir zunächst: Ist $\mathfrak{B}$ lokal kongruent in sich, so gilt folgendes:

a) Zu den auf $\mathfrak{B}$ beliebig gewählten Punkten P_1, P_2 gibt es (unendlich viele) Paare von *beliebig kleinen*, kongruenten Umgebungen $\mathfrak{U}(P_1;\mathfrak{B})$ und $\mathfrak{U}(P_2;\mathfrak{B})$. Denn *jede* in einer $\mathfrak{U}(P_1;B)$ enthaltene Umgebung von P_1 ist kongruentes Bild einer in $\mathfrak{U}(P_2;\mathfrak{B})$ enthaltenen Umgebung von P_2, wobei P_1 Bild von P_2 wird.

b) Wird mit E irgendeine kongruenzinvariante [3]) Eigenschaft lokaler Natur bezeichnet und kommt E dem Bogen $\mathfrak{B}$ in einem einzigen Punkte P' zu, so kommt E dem $\mathfrak{B}$ überhaupt in *jedem* Punkte zu.

---

[1]) Nach Mitteilung von Herrn Reinhardt ist diese Frage bei seinen Untersuchungen über Zerlegungsbereiche aufgetaucht: Über die Zerlegung der euklidischen Ebene in kongruente Bereiche, Sitz.-Ber. d. preuß. Akad. d. Wiss., physikal.-math. Klasse 1928, S. 26 ff., vgl. insbes. Fußnote 3, Seite 45.

[1a]) Man beachte die (in der Schreibweise nicht zum Ausdruck kommende) Abhängigkeit von $\mathfrak{U}(P_1;\mathfrak{M})$ nnd $\mathfrak{U}(P_2;\mathfrak{M})$ bzw. von $\mathfrak{U}(P_1)$ und $\mathfrak{U}(P_2)$.

[2]) Unter einem *Jordanbogen* oder *einfachen* Bogen $\mathfrak{B}$ verstehen wir hierbei nicht das topologische Bild $\overline{\mathfrak{B}}$ einer abgeschlossenen Strecke, sondern das in $\overline{\mathfrak{B}}$ enthaltene *Bild des offenen Kerns der Strecke.*

[3]) d. h. invariant gegenüber beliebigen kongruenten Transformationen.

2, 1. Wir erledigen zuerst den Fall, daß $\mathfrak{B}$ lokal in sich kongruent ist und *Strecken als Teilbogen* enthält. Ist P' innerer Punkt einer solchen Teilstrecke, besitzt er also eine geradlinige Umgebung, so besitzt (vgl. Nr. 2, b) *jeder* Punkt P von $\mathfrak{B}$ eine Strecke als Umgebung auf $\mathfrak{B}$. Jeder abgeschlossene Teilbogen $\mathfrak{B}'$ von $\mathfrak{B}$ kann folglich (wegen der Kompaktheit von $\mathfrak{B}'$) mit endlich vielen Strecken völlig überdeckt werden, muß also selbst eine Strecke sein. *Ohne Beschränkung der Allgemeinheit kann daher angenommen werden, daß $\mathfrak{B}$ keine Teilstrecken enthält.*

2, 2. Wir beweisen jetzt, daß jeder lokal in sich kongruente Jordanbogen $\mathfrak{B}$ (mindestens) *einen konvexen Teilbogen enthält.* Zu dem Zwecke bezeichnen wir [4]) als *Punkt mit Stützstrecken an* $\mathfrak{B}$ jeden Punkt P^* von $\mathfrak{B}$, zu welchem eine abgeschlossene Halbkreisscheibe $\mathfrak{H} = \mathfrak{H}(P^*)$ mit dem Zentrum P^* gehört von folgender Eigenschaft: Alle Punkte des Durchschnittes $\mathfrak{H} \frown \mathfrak{B}$ liegen auf dem Durchmesser d, von welchem $\mathfrak{H}$ begrenzt wird. Diesen Durchmesser nennen wir eine *Stützstrecke* in P^* an $\mathfrak{B}$; mit d ist auch jede beliebig kleine in d enthaltene, von P^* halbierte Strecke eine Stützstrecke in P^* an $\mathfrak{B}$. Nun liegen in jedem Falle auf dem einfachen Bogen $\mathfrak{B}$ die Punkte mit Stützstrecken dicht [5]) (also auch dann, wenn $\mathfrak{B}$ keinen konvexen Teilbogen enthalten sollte). Es sei daher P^* ein Punkt mit Stützstrecken an $\mathfrak{B}$. Wegen Nr. 2, b) ist dann überhaupt *jeder* Punkt P von $\mathfrak{B}$ ein Punkt mit Stützstrecken an $\mathfrak{B}$; m. a. W.: Es gibt auf $\mathfrak{B}$ keinen Punkt ohne Stützstrecken an $\mathfrak{B}$. Dann aber muß $\mathfrak{B}$ konvexe Teilbogen enthalten [6]), wie behauptet.

2, 3. Es sei $\mathfrak{K}$ ein konvexer Teilbogen des lokal in sich kongruenten Jordanbogens $\mathfrak{B}$ und P_1 ein auf $\mathfrak{K}$ innerer Punkt von $\mathfrak{K}$. *Jede* hinreichend kleine Umgebung von P_1 auf $\mathfrak{B}$ ist dann ebenfalls konvex. Zufolge Nr. 2, b) besitzt also überhaupt jeder Punkt P von $\mathfrak{B}$ eine konvexe Umgebung $\mathfrak{P} = \mathfrak{B}(P; \mathfrak{B})$ auf $\mathfrak{B}$, d. h. $\mathfrak{B}$ ist „*konvex im Kleinen*". Wegen der Konvexität von $\mathfrak{K}$ liegen auf $\mathfrak{K}$ gewöhnlich differenzierbare Punkte P_1' dicht, d. h. solche Punkte, in welchen $\mathfrak{K}$ keine Ecke besitzt. Daher ist überhaupt *jeder* Punkt von $\mathfrak{B}$ gewöhnlich differenzierbar. Wegen der Konvexität von $\mathfrak{B}$ im Kleinen folgt aber aus der Existenz der Tangente ohne weiteres die Stetigkeit der Tangente. Es besitzt daher $\mathfrak{B}$ in *jedem* Punkte sogar eine *stetige* Tangente.

2, 4. Es sei nun $\mathfrak{P}$ wieder eine konvexe hinreichend kleine Umgebung von P auf $\mathfrak{B}$ und $\mathfrak{B}$ wieder lokal in sich kongruent. Bei passender Wahl (rechtwinkliger) kartesischer Koordinaten ist dann $\mathfrak{P}$ darstellbar durch $y = f(x)$, mit $a \leqq x \leqq b$, wo $f(x)$ konvex und stetig differenzierbar ist in $[a, b]$. Folglich besitzt die (stetige) monotone Funktion $f'(x)$ fast überall in $[a, b]$, also z. B. für $x = c$, eine *endliche* Ableitung [7]) und daher besitzt $f(x)$ eine endliche zweite Ableitung $f''(x)$, z. B. im Punkte C mit der Abszisse $x = c$. Bezogen auf jeweils passend gewählte Koordinaten ist daher auch $\mathfrak{B}$ in *jedem* Punkte P zweimal differenzierbar, besitzt also insbesondere in jedem Punkte eine eindeutig bestimmte, endliche Krümmung (im klassischen Sinne) gleich

$$\frac{f''}{(1 + f'^2)^{\frac{3}{2}}}.$$

Da die Krümmung kongruenzinvariant ist, so hat (zufolge Nr. 2, b)) $\mathfrak{B}$ in jedem Punkte P

[4]) Nach dem Vorgange von B. Kaufmann, Über die Konvexitäts- und Konkavitätsstellen auf Jordankurven, Crelles Journal **164** (1931), § 1, Nr. 1, S. 113.

[5]) Vgl. a. a. O. [4]), § 1, Nr. 2 (letzte Zeile), S. 114.

[6]) Vgl. a. a. O. [4]), § 4, Nr. 10, S. 122.

[7]) Vgl. z. B. Montel-Rosenthal, Integration und Differentiation, Enzyklopädie d. math. Wiss. IIC 9 b, S. 1092/93.

die gleiche endliche Krümmung k. Wäre $k = 0$, so wäre die Umgebung $\mathfrak{P}$ von P eine Strecke, gegen die in Nr. **2**, 1 getroffene Verabredung. Ist aber $k \neq 0$, so kann die Umgebung eines jeden Punktes auf $\mathfrak{B}$ nur ein Kreisbogen vom Radius $\frac{1}{k}$ sein [8]). Weil nun jeder abgeschlossene Teilbogen von $\mathfrak{B}$ mit endlich vielen derartigen Kreisbogen überdeckbar ist, muß $\mathfrak{B}$ selbst ein Kreisbogen von eben diesem Radius sein, w. z. b. w.

3. Zum Schlusse sei noch auf einige *Verallgemeinerungen* Ihrer Fragestellung hingewiesen, zu denen man bei den vorstehenden Betrachtungen von selbst geführt wird. Eine volle Erledigung dieser Verallgemeinerungen ist hier nicht beabsichtigt.

3, 1. Der im Vorangehenden angegebene Beweis Ihres Satzes ist in seinem ersten Teile (Nr. **2**, 1—**2**, 3) rein projektiver Natur.

Wir kommen so zu der etwas allgemeineren *Frage*: *Es sei $\mathfrak{B}$ ein lokal in sich projektiver* [9]) *Jordanbogen* (*in der Ebene*). *Ist $\mathfrak{B}$ Teilbogen einer ebenen Kurve, welche bei einer* (*eingliedrigen*) *Gruppe projektiver Transformationen in sich übergeht*?

Sicher ist jedenfalls, daß ein lokal in sich projektiver Bogen konvex im Kleinen (und in jedem Punkte zweimal differenzierbar) sein muß.

3, 2. Zur Ausdehnung unserer Frage auf den Raum R_3, allgemein auf den R_n, gelangen wir von der Bemerkung aus, daß Kreis und Gerade unter den z. B. zweimal stetig differenzierbaren ebenen Kurven gekennzeichnet sind durch die Konstanz der Krümmung. Im R_3 haben wir die Schraubenlinie als Kurve konstanter erster *und* zweiter Krümmung [10]). Allgemein können wir als *Schraubenbogen im R_n* jeden n-mal stetig differenzierbaren Bogen des R_n bezeichnen, längs dessen jede seiner $n-1$ Krümmungen konstant ist [11]). Man kommt so zur *Frage*: *Sind die Schraubenbogen des R_n gekennzeichnet durch lokale Kongruenz in sich*?

Läßt man nur n-mal stetig differenzierbare Bogen zur Konkurrenz zu, so ist diese Frage ohne weiteres zu bejahen; es folgt das aus der Bewegungsinvarianz der Krümmungen in Verbindung mit ihrer vorausgesetzten Stetigkeit. — Die Behandlung des allgemeinen Falles, also ohne Differenzierbarkeitsannahmen, würde entsprechend wie im Falle des R_2 gelingen, wenn man zeigen könnte: 1. jeder lokal in sich kongruente Bogen enthält einen Bogen n-ter Ordnung; 2. dieser Bogen n-ter Ordnung ist n-mal stetig differenzierbar; hierbei wären u. a. die bekannten Differenzierbarkeitseigenschaften der Bogen n-ter Ordnung heranzuziehen.

Weitere Verallgemeinerungen liegen auf der Hand.

---

[8]) Wie man etwa durch Auflösung der Differentialgleichung $kf'' = (1 + f'^2)^{3/2}$ leicht bestätigt.

[9]) $\mathfrak{B}$ heißt *lokal in sich projektiv*, wenn zu irgend zweien seiner Punkte P_1, P_2 Umgebungen $\mathfrak{U}(P_1; \mathfrak{B})$ und $\mathfrak{U}(P_2; \mathfrak{B})$ existieren, welche projektiv so aufeinander abgebildet werden können, daß P_1 und P_2 einander entsprechen.

[10]) Vgl. Duschek-Mayer, Lehrbuch der Differentialgeometrie **1**, Leipzig und Berlin, 1930, S. 49 und 77. — Ist die zweite Krümmung Null, so haben wir Kreis oder Gerade.

[11]) Unter den „Krümmungen" $k_1, \ldots, k_{n-1}$ des betrachteten Bogens $\mathfrak{B}$ verstehen wir die Koeffizienten seiner „natürlichen" Gleichungen (Frenetformeln). Ist s der kleinste Index, für welchen $k_s = 0$, so liegt $\mathfrak{B}$ in einem s-dimensionalen linearen Unterraum des R_n, aber in keinem niedrigerdimensionalen. Vgl. a. a. O. [10]) **2**, S. 72 ff.

Eingegangen 13. Juli 1935.

Über die Darstellungen endlicher Gruppen.

Von *Otto F. G. Schilling* in Apolda.

I. Schur [1]) hat die Vermutung ausgesprochen, daß die absolut-irreduziblen Darstellungen einer endlichen Gruppe der Ordnung n schon im Körper der n-ten Einheitswurzeln möglich sind. Für Gruppen von Primzahlpotenzordnung $n = p^\nu$ kann die Richtigkeit dieser Vermutung ohne weiteres der bekannten Tatsache entnommen werden, daß für diese Gruppen sämtliche Darstellungen monomial sind [2]).

Der nachfolgend gegebene einfache arithmetische Beweis der Schurschen Vermutung für Gruppen von Primzahlpotenzordnung ist aber vielleicht doch nicht ohne Interesse, weil er ein Wegweiser für einen Beweis im allgemeinen Falle sein kann.

Satz. *Die absolut-irreduziblen Darstellungen einer endlichen Gruppe* $\mathfrak{G}$ *von Primzahlpotenzordnung* p^ν *sind im Körper* k *der* p^ν*-ten Einheitswurzeln möglich.*

Beweis. Wir betrachten den Gruppenring $\mathfrak{G}_k = \sum_{S \text{ in } \mathfrak{G}} Sk$ von $\mathfrak{G}$ über k als Koeffizientenbereich. Ist $\mathfrak{o}$ die Hauptordnung von k, so ist $\mathfrak{G}_\mathfrak{o} = \sum_{S \text{ in } \mathfrak{G}} S\mathfrak{o}$ eine Ordnung von $\mathfrak{G}_k$. Die Diskriminante von $\mathfrak{G}_\mathfrak{o}$ ist bekanntlich $(p^\nu)^{p^\nu}$ [3]). Daher ist die Diskriminante (einer Maximalordnung) von $\mathfrak{G}_k$ als Teiler von $(p^\nu)^{p^\nu}$ eine Potenz des einzigen Primteilers $\mathfrak{p}$ von p in k. Insbesondere ist diese Diskriminante nicht Null, und daher ist $\mathfrak{G}_k$ halbeinfach, also direkte Summe einfacher Algebren A_i über k. Die Zentren der A_i entstehen aus k durch Adjunktion der Charaktere der verschiedenen absolut-irreduziblen Darstellungen von $\mathfrak{G}$. Da diese Charaktere sämtlich in k liegen, ist k selbst Zentrum aller A_i, d. h. die A_i sind normale einfache Algebren über k. Die Diskriminanten der A_i sind als Teiler der Diskriminante von $\mathfrak{G}_k$ Potenzen von $\mathfrak{p}$. Da k total-imaginär ist — der triviale Fall $p^\nu = 2^1$ kann beiseite gelassen werden —, haben also die A_i sämtlich höchstens die *eine* Verzweigungsstelle $\mathfrak{p}$. Nach der arithmetischen Theorie der normalen einfachen Algebren über einem algebraischen Zahlkörper geht das aber nur, wenn die A_i über k zerfallen, da sonst mindestens *zwei* verschiedene Verzweigungsstellen vorhanden sein müssen [4]). Daher ist k Zerfällungskörper für alle A_i. Das läuft auf die Behauptung hinaus.

---

[1]) I. Schur, Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen, Berl.-Ber. 1906.

[2]) A. Speiser, Gruppentheorie (2. Aufl., Berlin 1927), Satz 169.

[3]) Hierzu und zu den folgenden Feststellungen siehe E. Noether, Hyperkomplexe Größen und Darstellungstheorie, Math. Zeitschr. **30** (1929), §§ 24, 26, oder B. L. van der Waerden, Moderne Algebra II (Berlin 1931), Kap. 17.

[4]) Siehe hierzu H. Hasse, Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper, Math. Ann. **107** (1933), Satz (6. 54).

Eingegangen 26. August 1935.

Zur Theorie der komplexen Multiplikation. I.

Von *Masao Sugawara* in Tokyo.

In der Begründung der Theorie der komplexen Multiplikation von Herrn Hasse [1]) ist die Frage, ob sich jeder relativ abelsche Körper über einem imaginär quadratischen Zahlkörper Ω allein durch einen singulären Wert der Weberschen τ-Funktion erzeugen läßt, offen geblieben. Nach Herrn Hasse ist nämlich

$$K_{\mathfrak{m}} = \Omega(\tau(\mathfrak{k}^*), j(\mathfrak{k}))$$

der Strahlklassenkörper mod $\mathfrak{m}$ über Ω; über $\Omega(\tau(\mathfrak{k}^*))$ aber war bisher nichts bekannt. Im folgenden beweise ich, daß

$$K_{\mathfrak{m}} = \Omega(\tau(\mathfrak{k}^*)),$$

unter der Voraussetzung allerdings, daß $\mathfrak{m}$ ein echtes Multiplum von 4 ist [2]). Ich vermute, daß die Behauptung allgemein gilt und daß die Voraussetzung nur durch die Beweismethode bedingt ist. Jedenfalls läßt sich über den sogenannten Kroneckerschen Jugendtraum folgendes Resultat aussprechen: *Jeder relativ abelsche Körper über Ω ist in einem Körper enthalten, der aus Ω durch Adjunktion einer Zahl $\tau(\mathfrak{k}^*)$ entsteht.*

Der Beweis wird in §§ 1, 2 zunächst unter voller Benutzung der Hasseschen Theorie geführt. In § 3 wird gezeigt, daß man bei Anwendung des Satzes von der verallgemeinerten arithmetischen Progression die Resultate von H. II, insbesondere das Prinzip der komplexen Multiplikation, nicht zu benutzen braucht; die Hassesche Theorie erfährt dann eine gewisse Vereinfachung.

§ 1. Für jede Strahlklasse $\mathfrak{k}^*$ mod $\mathfrak{m}$ ist der Körper $\Omega(\tau(\mathfrak{k}^*))$ als Teilkörper des über Ω abelschen Körpers $K_{\mathfrak{m}}$ selbst abelsch, also sicher galoissch über Ω. Da die Gesamtheit der $\tau(\mathfrak{k}^*)$ ein volles System von Konjugierten über Ω bildet (H. II, Satz 21), sind alle $\tau(\mathfrak{k}^*)$ in jedem $\Omega(\tau(\mathfrak{k}^*))$ enthalten, und man erhält denselben Körper, gleichviel ob man eine oder sämtliche Strahlklasseninvarianten mod $\mathfrak{m}$ zu Ω adjungiert. Daher genügt es zu zeigen, daß die absolute Klasseninvariante $j(\mathfrak{k})$ rational durch die sämtlichen Strahlklasseninvarianten mod $\mathfrak{m}$ darstellbar ist.

§ 2. Nunmehr setze ich voraus, daß $\Omega \neq P(\sqrt{-1}), P(\sqrt{-3})$, was erlaubt ist, da in diesen beiden Körpern die Klassenzahl gleich 1 und daher die Behauptung evident ist. Es sei $4 \mid \mathfrak{m}$, $\mathfrak{m} \neq 4$ und $\tau(\mathfrak{k}^*) = \tau(\varrho \mid \mathfrak{a})$ eine Strahlklasseninvariante. Es gibt genau vier mod $\mathfrak{m}$ inkongruente durch $\frac{\mathfrak{m}}{2}$ teilbare ganze Zahlen $\omega_0 \equiv 0 \bmod^+ \mathfrak{m}$, $\omega_1, \omega_2, \omega_3$. Für die Zahlen $\tau_i = \tau((1+\omega_i)\varrho \mid \mathfrak{a})$ $(i = 0, 1, 2, 3)$ gilt:

[1]) H. Hasse, Neue Begründung der komplexen Multiplikation I, II; Journ. f. reine u. angew. Math. **157** (1927), **165** (1931); im folgenden zitiert als H. I, H. II. Die vorliegende Note schließt sich an diese Arbeiten an. Von den dortigen Bezeichnungen mache ich ohne nochmalige Erklärung Gebrauch.

[2]) Meine frühere Note, On the So-called Kronecker's Dream in Youngdays (Proc. Phys.-Math. Soc. of Japan **15** (1933)), worin ich einen ähnlichen Satz beweisen wollte, enthält ein Versehen.

(1) Die τ_i sind Strahlklasseninvarianten mod $\mathfrak{m}$.

(2) $\tau_i \neq \tau_j$, wenn $i \neq j$.

(1) folgt daraus, daß $1 + \omega_i$ wegen $4 | \mathfrak{m}$ prim zu $\mathfrak{m}$ ist, $(1 + \omega_i)\varrho$ also von der Form $\frac{\mathfrak{r}_i \mathfrak{a}}{\mathfrak{m}}$ mit ganzem zu $\mathfrak{m}$ primem $\mathfrak{r}_i$ ist. Wenn (2) falsch wäre, folgte

$$(1 + \omega_i)\varrho \equiv \pm (1 + \omega_j)\varrho \bmod^+ \mathfrak{a}, \qquad 1 + \omega_i \equiv \pm (1 + \omega_j) \bmod^+ \mathfrak{m}.$$

$\omega_i \equiv \omega_j$ ist gegen die Wahl der ω_i; $1 + \omega_i \equiv -(1 + \omega_j)$ ist ebenfalls unmöglich, da sonst $\frac{\mathfrak{m}}{2}$ in 2, also $\mathfrak{m}$ in 4 aufginge. Ferner sind die drei Zahlen $\omega_1\varrho$, $\omega_2\varrho$, $\omega_3\varrho$ drei verschiedene Halbperioden der Funktion $\tau(u | \mathfrak{a})$, da sie einerseits $\bmod^+ \mathfrak{a}$ inkongruent sind, andererseits bei Verdoppelung $\equiv 0 \bmod^+ \mathfrak{a}$ werden.

Das Additionstheorem der Weierstraßschen $\wp$-Funktion für ein beliebiges Argument u und eine Halbperiode h lautet wegen $\wp'(h) = 0$

$$4(\wp(u + h) + \wp(u) + \wp(h))\,(\wp(u) - \wp(h))^2 = \wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u) - g_3$$

und auf $\tau(u) = \tau(u | \mathfrak{a})$ umgerechnet (über den Zusammenhang mit $\wp(u)$ siehe H. I, Seite 127)

$$(\tau(u + h) + \tau(u) + \tau(h))\,(\tau(u) - \tau(h))^2 = \tau(u)^3 - A\tau(u) + B,$$

wobei $A = 3j(\mathfrak{a})\,(j(\mathfrak{a}) - 2^6 3^3)$, $B = 2j(\mathfrak{a})\,(j(\mathfrak{a}) - 2^6 3^3)^2$. Darin werde eingeführt $h = \omega_1\varrho$, $u = (1 + \omega_i)\varrho$, also $\tau(u) = \tau_i$. Dann folgt, wenn $\tau(u + h) = \tau((1 + \omega_i + \omega_1)\varrho | \mathfrak{a}) = \overline{\tau}_i$ gesetzt wird,

$$(*) \qquad (\overline{\tau}_i + \tau_i + \tau(h))\,(\tau_i - \tau(h))^2 = \tau_i^3 - A\tau_i + B.$$

Dabei ist $\overline{\tau}_0 = \tau_1$, $\overline{\tau}_1 = \tau_0$, und wegen $\omega_1 + \omega_2 \equiv \omega_3 \bmod^+ \mathfrak{m}$ ferner $\overline{\tau}_2 = \tau_3$, $\overline{\tau}_3 = \tau_2$. Die Auflösung der Klammern ergibt vier lineare inhomogene Gleichungen für die zu bestimmenden Zahlen

$$\tau(h)^3 - B, \quad A, \quad \tau(h)^2, \quad -\tau(h)$$

mit der Determinante

$$\begin{vmatrix} 1 & \tau_0 & \tau_1 - \tau_0 & (2\tau_1 + \tau_0)\tau_0 \\ 1 & \tau_1 & \tau_0 - \tau_1 & (2\tau_0 + \tau_1)\tau_1 \\ 1 & \tau_2 & \tau_3 - \tau_2 & (2\tau_3 + \tau_2)\tau_2 \\ 1 & \tau_3 & \tau_2 - \tau_3 & (2\tau_2 + \tau_3)\tau_3 \end{vmatrix} = (\tau_0 + \tau_1 - \tau_2 - \tau_3)^2\,(\tau_0 - \tau_1)\,(\tau_2 - \tau_3).$$

Der erste Faktor ist von Null verschieden, denn wenn $\tau_0 + \tau_1 = \tau_2 + \tau_3 = \sigma$ wäre, so folgte aus (*), daß die Gleichung dritten Grades für die τ_i

$$(\sigma + \tau(h))\,(\tau_i - \tau(h))^2 = \tau_i^3 - A\tau_i + B$$

die vier verschiedenen Wurzeln τ_i hätte. Da auch die beiden anderen Faktoren nicht Null sind, läßt sich das Gleichungssystem im Körper $\Omega(\tau(\mathfrak{k}^*))$ auflösen. Daher ist

$$j(\mathfrak{a}) = \frac{3B}{2A} + 2^6 3^3$$

in $\Omega(\tau(\mathfrak{k}^*))$ enthalten, wie zu zeigen war. Es ist also bewiesen:

Es sei $4 | \mathfrak{m}$, $\mathfrak{m} \neq 4$ *und* $\tau(\mathfrak{k}^*)$ *eine Strahlklasseninvariante* mod $\mathfrak{m}$; *dann ist* $\Omega(\tau(\mathfrak{k}^*))$ *der Strahlklassenkörper* mod $\mathfrak{m}$ *über* Ω.

§ 3. Das eben bewiesene Resultat soll jetzt noch einmal ohne Benutzung der Theorie von H. II, also insbesondere ohne das Prinzip der komplexen Multiplikation, abgeleitet werden. Dabei wird über die Klasseninvarianten $j(\mathfrak{k})$, $\tau(\mathfrak{k}^*)$ nur ihre Definition, die einfachen Verschiedenheitsaussagen aus H. I und die fundamentale Kongruenz

$$\tau(\mathfrak{k}^*)^p \equiv \tau(\mathfrak{k}^* \mathfrak{k}_\mathfrak{p}^*) \bmod \mathfrak{p}$$

für die Primideale $\mathfrak{p}$ ersten Grades mit den in H. I, Satz 23 angegebenen endlich vielen Ausnahmen gebraucht.

Nach dem Satz von der verallgemeinerten arithmetischen Progression kann man jede Strahlklasse mod $\mathfrak{m}$ durch eins der angegebenen Primideale $\mathfrak{p}$ repräsentieren. Es sei nun für eine zunächst feste Strahlklasse $\mathfrak{k}^*$ vorausgesetzt

$$(**) \qquad \tau(\mathfrak{k}^*) = \tau(\mathfrak{k}^* \mathfrak{k}_\mathfrak{p}^*).$$

Für eine andere, $\mathfrak{k}^* \mathfrak{k}_\mathfrak{q}^*$, folgt dann aus der obigen Kongruenz

$$\tau(\mathfrak{k}^*)^q \equiv \tau(\mathfrak{k}^* \mathfrak{k}_\mathfrak{q}^*), \quad \tau(\mathfrak{k}^* \mathfrak{k}_\mathfrak{p}^*)^q \equiv \tau(\mathfrak{k}^* \mathfrak{k}_\mathfrak{p}^* \mathfrak{k}_\mathfrak{q}^*),$$

also

$$\tau(\mathfrak{k}^* \mathfrak{k}_\mathfrak{q}^*) \equiv \tau(\mathfrak{k}^* \mathfrak{k}_\mathfrak{q}^* \mathfrak{k}_\mathfrak{p}^*) \mod \mathfrak{q}.$$

Da das für unendlich viele $\mathfrak{q}$ gilt, folgt $\tau(\mathfrak{k}^* \mathfrak{k}_\mathfrak{q}^*) = \tau(\mathfrak{k}^* \mathfrak{k}_\mathfrak{q}^* \mathfrak{k}_\mathfrak{p}^*)$. Gleichung (**) gilt also für alle Strahlklassen $\mathfrak{k}^*$.

Nun ist

$$\tau(\mathfrak{k}^*) = \tau(\varrho | \mathfrak{a}), \quad \tau(\mathfrak{k}^* \mathfrak{k}_\mathfrak{p}^*) = \tau\left(\varrho \middle| \frac{\mathfrak{a}}{\mathfrak{p}}\right).$$

Ist ξ ganz und zu $\mathfrak{m}$ prim, so ist $\tau(\xi\varrho | \mathfrak{a}) = \tau(\mathfrak{k}^* \mathfrak{k}_1^*)$ eine andere zur gleichen absoluten Idealklasse wie $\mathfrak{k}^*$ gehörige Strahlklasse mod $\mathfrak{m}$, und $\tau(\mathfrak{k}^* \mathfrak{k}_1^* \mathfrak{k}_\mathfrak{p}^*) = \tau\left(\xi\varrho \middle| \frac{\mathfrak{a}}{\mathfrak{p}}\right)$. Nach dem eben Festgestellten ist daher

$$\tau(\xi\varrho | \mathfrak{a}) = \tau\left(\xi\varrho \middle| \frac{\mathfrak{a}}{\mathfrak{p}}\right).$$

Durch die Methode von § 2 ergibt sich daraus, da die Zahlen ω_i nicht von $\mathfrak{a}$ abhängig sind,

$$j(\mathfrak{a}) = j\left(\frac{\mathfrak{a}}{\mathfrak{p}}\right).$$

Da die absoluten Klasseninvarianten sämtlich voneinander verschieden sind (H. I, Satz 6), liegt also $\mathfrak{p}$ in der absoluten Hauptklasse. Da die Strahlklasseninvarianten, die zur selben absoluten Idealklasse gehören, sämtlich voneinander verschieden sind (H. I, Satz 20), gehört $\mathfrak{p}$ nach (**) sogar zum Strahl mod $\mathfrak{m}$. Die sämtlichen Strahlklasseninvarianten mod $\mathfrak{m}$ sind daher voneinander verschieden. Aus dieser Tatsache ergibt sich nach dem Vorbild von H. I, Satz 24 ohne weiteres das Zerlegungsgesetz von $\Omega(\tau(\mathfrak{k}^*))$, und zwar das Klassenkörperzerlegungsgesetz für den Strahlklassenkörper mod $\mathfrak{m}$. Damit ist das Resultat von § 2 auch auf diesem Wege erreicht.

Bei der Redaktion dieser Arbeit haben mir die Herren Franz und Iyanaga geholfen; ich möchte ihnen meinen herzlichen Dank aussprechen.

Eingegangen 29. März 1935.

Der Euklidische Algorithmus in quadratischen Körpern.

Von *H. Behrbohm* und *L. Rédei* in Göttingen.

Existiert in einem absolut quadratischen Zahlkörper $K(\sqrt{m})$, m ganz rational, quadratfrei, zu je zwei ganzen Zahlen α und $\beta \neq 0$ eine dritte ganze Zahl γ derart, daß

$$|N(\alpha - \beta\gamma)| < |N(\beta)|$$

ist, so sagen wir, $K(\sqrt{m})$ besitze den Euklidischen Algorithmus, kurz: den E. A.

Unter den imaginären $K(\sqrt{m})$ haben nach Dickson[1]) genau die fünf Körper mit $m = -1, -2, -3, -7, -11$ den E. A. Bei den reellen $K(\sqrt{m})$ existiert der E. A. für $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41$. Bis auf $m = 19$ und die drei letzten von Oppenheim[2]) und Remak[3]) behandelten Fälle geht dies auf Perron[4]) zurück. $m = 19$ wurde von Berg[5]) behandelt; derselbe bewies auch, daß im Falle $m \not\equiv 1 \pmod 4$ außer den hier genannten Körpern keine weiteren mit E. A. existieren, nachdem schon Hofreiter[6]) die Restklasse 14 (mod 24), Oppenheim die Fälle $m = 23, 31$ erledigt hatte. Letzterer bewies die Nichtexistenz auch für $m = 53$, welcher Fall unter die hier folgenden allgemeineren Resultate fällt.

In dieser Arbeit, deren Resultate uns größtenteils schon im Oktober 1934 bekannt waren, bringen wir u. a. nochmals Beweise für die Resultate Bergs. Es scheint uns nämlich, daß wir das Problem allgemeiner in Angriff genommen haben, als dies bis jetzt geschah. Denn zunächst setzen wir auseinander, welche Fälle von vorneherein nur in Frage kommen können. Dies geschieht in **1**. Dann aber greifen wir auch alles von einem umfassenden Gesichtspunkt aus an durch Aufstellung eines Hilfssatzes in **2**, auf dem alle Nichtexistenzbeweise des E. A. im folgenden beruhen. So können wir in **3** und **4** kürzer als Berg den Fall $m \not\equiv 1 \pmod 4$ erledigen. In **5** wird $m = 19$ diskutiert. Im Gegensatz zu Berg führen wir dies detailliert aus, da der Existenzbeweis für diesen Fall schwieriger ist als für die übrigen oben genannten Fälle. Unser Beweis ist ökonomischer als der Bergsche, da bei uns nur zehn Koordinatenpaare, bei Berg aber deren fünfzehn benötigt werden.

Die Abschnitte **6** bis **10** beschäftigen sich mit dem Fall $m \equiv 1 \pmod 4$. In **6** stellen wir nämlich einen allgemeinen Satz auf, mit dessen Hilfe man in gewissen Fällen auf

---

[1]) L. E. Dickson, Algebren und ihre Zahlentheorie, Zürich 1927, S. 151.

[2]) A. Oppenheim, Quadratic fields with and without Euclid's algorithm, Math. Annalen **109** (1934), S. 349—352.

[3]) R. Remak, Über den euklidischen Algorithmus in reell-quadratischen Zahlkörpern, Jahresbericht d. D. M. V. **44** (1934), S. 238—250.

[4]) O. Perron, Quadratische Zahlkörper mit Euklidischem Algorithmus, Math. Annalen **107** (1932), S. 489—495.

[5]) E. Berg, Über die Existenz eines Euklidischen Algorithmus in quadratischen Zahlkörpern, Kungl. Fysiografiska Sällskapets i Lund Förhandlingar **5** (1935), Nr. 5.

[6]) N. Hofreiter, Quadratische Zahlkörper ohne Euklidischen Algorithmus, Math. Annalen **110** (1935), S. 194 bis 196.

die Nichtexistenz des E. A. schließen kann. In **7** ziehen wir aus diesem Satz eine interessante Folgerung als Vorbereitung für die Entwicklungen in **8** und **9**. Es sei $m = pq$ das Produkt der beiden Primzahlen p und q, $p \equiv q \equiv 3 \pmod 4$, $3 < p < q$. Dann bringt **8** im Falle des Bestehens des E. A. in $K(\sqrt{m})$ eine Abschätzung von $\frac{q}{p}$ nach oben, die für $p > 2500$ insbesondere $q < 2p$ liefert. **9** dagegen lehrt, daß in $K(\sqrt{m})$ der E. A. nicht existiert, falls überdies $m \equiv 5 \pmod 8$ ist[7]). In **10** wird unmittelbar auf Grund von **6** gezeigt, daß außer den erwähnten $m = 5$ und $m = 29$ keine weiteren Primzahlen der Klasse 5 (mod 24) zu einem $K(\sqrt{m})$ mit E. A. führen.

1. Existiert in $K(\sqrt{m})$ der E. A., so hat $K(\sqrt{m})$ die Klassenzahl 1. Wir bezeichnen mit p, q durchweg positive Primzahlen und beweisen:

Hat $K(\sqrt{m})$ die Klassenzahl 1, so sind nur die folgenden Fälle möglich:

I. $m = p \equiv 1 \pmod 4$

II. $m = pq \equiv 1 \pmod 4$, $p \equiv q \equiv 3 \pmod 4$

III. $m = 2$ oder $m = 2p$, $p \equiv 3 \pmod 4$

IV. $m = p \equiv 3 \pmod 4$.

Sei nämlich D die Diskriminante von $K(\sqrt{m})$, d. h. $D = m$ bzw. $4m$, je nachdem $m \equiv 1$ oder $\not\equiv 1 \pmod 4$ ist. Es bezeichne weiter h die Klassenzahl des Körpers im gewöhnlichen Sinne und h_0 die im engeren Sinne. Dann ist $h = \frac{h_0}{2}$ dann und nur dann, wenn für die Grundeinheit ε des Körpers $N(\varepsilon) = +1$ gilt, sonst ist stets $h_0 = h$. Es ist $2^{e_2+e_4} \mid h_0$, wobei e_i $(i = 2, 4)$ die Anzahl der durch i teilbaren Invarianten der absoluten im engeren Sinne genommenen Klassengruppe des Körpers ist. Es folgt also $2^{e_2+e_4-x} \mid h$, wobei $x = 0$ oder 1 ist, je nachdem ob $N(\varepsilon) = -1$ oder $+1$ ist. Ist daher $h = 1$, so muß $e_2 + e_4 - x = 0$ sein. Dann ist aber nur $e_2 = 0$ $(e_4 = x = 0)$ oder $e_2 = 1, e_4 = 0, x = 1$ möglich. Nach einem Gaußschen Satze ist $e_2 = \nu - 1$, wo unter ν die Anzahl der verschiedenen Primfaktoren von D verstanden wird; im ersten Falle ist also D eine Primzahlpotenz, m eine Primzahl. Im zweiten Falle hat D genau zwei verschiedene Primteiler. D läßt sich dann eindeutig als Produkt $D_1 D_2$ darstellen, wobei auch D_1, D_2 Diskriminantenzahlen sind, die die Gestalt $-4, 8, -8, p$ oder $-p$ haben. Im Sinne von Rédei[8]) ist jetzt D_1, D_2 die einzige eigentliche D-Zerfällung. D_1 und D_2 können nicht beide positiv sein. Dann würde nämlich aus dem Satze von Rédei[9]) bzw. Dirichlet[9]) folgen, daß $e_4 = 1$ bzw. $x = 0$ ist, je nachdem die D-Zerfällung D_1, D_2 von der zweiten Art ist oder nicht. Dies ist aber nach dem Vorigen unmöglich. Im Falle eines zusammengesetzten D müssen also D_1 und D_2 beide negativ sein, d. h. es muß $D = (-4)(-p)$ oder $(-8)(-p)$ oder $(-p)(-q)$ sein mit $p \equiv q \equiv 3 \pmod 4$.

2. Nach Perron läßt sich die Bedingung für den E. A. so umgestalten:

Im Körper $K(\sqrt{m})$ existiert der E. A. dann und nur dann, wenn für jedes rationale Zahlenpaar a, b im Falle $m \not\equiv 1 \pmod 4$ die Ungleichung

$$|(x-a)^2 - m(y-b)^2| < 1\,, \tag{1}$$

im Falle $m \equiv 1 \pmod 4$ dagegen die Ungleichung

---

[7]) Nach einer brieflichen Mitteilung kann Herr Berg dies auch beweisen.

[8]) L. Rédei und H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, dieses Journal **170** (1933), S. 70.

[9]) A. a. O. [8]), S. 73 bzw. 74.

$$(2) \qquad \left|\left(\frac{x}{2}-a\right)^2 - m\left(\frac{y}{2}-b\right)^2\right| < 1 \qquad (x \equiv y \pmod 2)$$

in ganzen rationalen Zahlen x, y lösbar ist.

Wir bezeichnen mit r eine ganze rationale Zahl, für die $0 < r < m$ gilt und für die überdies die Kongruenz

$$(3) \qquad x^2 \equiv r \pmod m$$

mit ganzem rationalen x lösbar ist. Sei z eine solche Lösung von (3). Indem wir $a = 0$, $b = \frac{z}{m}$ setzen, erhalten wir aus (1) und (2) nach Multiplikation mit m bzw. $4m$

$$(1') \qquad |mx^2 - (my - z)^2| < m$$

und

$$(2') \qquad |mx^2 - (my - 2z)^2| < 4m \qquad (x \equiv y \pmod 2).$$

Wegen $mx^2 - (my - z)^2 \equiv -r \pmod m$ kann die linke Seite von (1') nur die Werte $-r$ oder $m - r$ annehmen. Analog ist wegen $mx^2 - (my - 2z)^2 \equiv -4r \pmod{4m}$ die linke Seite von (2') nur der Werte $-4r$ oder $4m - 4r$ fähig. Setzen wir also $y_1 = my - z$ bzw. $y_1 = my - 2z$, so haben wir den folgenden

Hilfssatz. *Existiert im Körper $K(\sqrt{m})$ der E. A. und bedeutet r eine Zahl $0 < r < m$, für die (3) lösbar ist, so muß im Falle $m \not\equiv 1 \pmod 4$ eine der beiden Gleichungen*

$$(1'') \qquad mx^2 - y_1^2 = -r \text{ oder } mx^2 - y_1^2 = m - r,$$

im Falle $m \equiv 1 \pmod 4$ dagegen eine der beiden Gleichungen

$$(2'') \qquad mx^2 - y_1^2 = -4r \text{ oder } mx^2 - y_1^2 = 4(m - r) \qquad (x \equiv y_1 \pmod 2)$$

in ganzen rationalen Zahlen x, y_1 lösbar sein.

3. Wir betrachten zuerst den Fall $m \equiv 2 \pmod 4$. Da $m = 2$ erledigt ist, können wir nach dem in **1** Gesagten $m = 2p$ mit $p \equiv 3 \pmod 4$ setzen. Hat r die Bedeutung aus **2** und ist dabei $r \equiv 5 \pmod 8$, so ist (mit Jacobischen Symbolen)

$$\left(\frac{m}{r}\right) = \left(\frac{2}{r}\right)\left(\frac{p}{r}\right) = -\left(\frac{r}{p}\right) = -1.$$

Außerdem ist wegen $m - r = 2p - r \equiv 1 \pmod 8$ auch

$$\left(\frac{m}{m-r}\right) = \left(\frac{2}{m-r}\right)\left(\frac{p}{m-r}\right) = \left(\frac{2p-r}{p}\right) = \left(\frac{-r}{p}\right) = -1.$$

Sowohl r als auch $m - r$ enthalten daher je mindestens einen Primzahlfaktor in ungerader Potenz, von dem m kein quadratischer Rest ist. Die Gleichungen (1'') können also nicht bestehen, da sie nicht einmal als Kongruenzen mod r bzw. mod $(m - r)$ bestehen können. Wir haben somit festgestellt:

Im Falle $m \equiv 2 \pmod 4$ kann in $K(\sqrt{m})$ der E. A. nur dann existieren, wenn alle ganzen Zahlen $\equiv 5 \pmod 8$ im Intervall $0, 2p$ quadratische Nichtreste mod p sind.

Wann kann dies nun eintreten? Es sei zunächst $p \equiv 3 \pmod 8$ und $p > 16$. Dann gibt es eine ganze rationale Zahl A mit $\frac{2p}{16} < A < \frac{3p}{16}$, für die sowohl $16A - p$ als auch $8A - p$ zwischen 0 und $2p$ liegen und $\equiv 5 \pmod 8$ sind. Wegen $\left(\frac{2}{p}\right) = -1$ ist aber die eine dieser beiden Zahlen quadratischer Rest mod p. Auch bei $p = 11$ ist 5 quadratischer Rest mod p. — Ist zweitens $p \equiv 7 \pmod 8$, $p > 16$, so gibt es ein ganzes rationales A mit $\frac{5p}{16} < A < \frac{6p}{16}$, für das jetzt die beiden Zahlen $16A - 5p$ und

$-8A+3p$ zwischen 0 und $2p$ liegen und $\equiv 5 \pmod 8$ sind. Wegen $\left(\frac{-2}{p}\right) = -1$ ist aber wieder die eine von ihnen quadratischer Rest mod p.

Zusammen mit den erwähnten, sich auf $m = 2, 6, 14$ beziehenden Resultaten von Perron und von Hofreiter haben wir daher den

Satz. *Im Falle* $m \equiv 2 \pmod 4$ *existiert in* $K(\sqrt{m})$ *der E. A. nur für* $m = 2$ *und* $m = 6$.

4. Es sei jetzt $m \equiv 3 \pmod 4$. Nach Nummer **1** beschränken wir uns auf den Fall $m = p \equiv 3 \pmod 4$ und wählen r in seiner Bedeutung aus Nummer **2** überdies so, daß $r \equiv -p+5 \pmod 8$ ist. Dann ist r durch 2, aber nicht durch 4 teilbar. Die Gleichung (1″) mit der rechten Seite $-r$ ist dadurch von vorneherein unmöglich. Denn x und y_1 müßten beide ungerade sein, so daß mod 8 die Kongruenz $p-1 \equiv -r$ folgen würde im Widerspruch zur Wahl von r. Es bleibt also nur noch übrig, die Gleichung (1″) mit der rechten Seite $m-r = p-r$ zu betrachten. Da jedoch

$$\left(\frac{m}{m-r}\right) = \left(\frac{p}{p-r}\right) = \left(\frac{p-r}{p}\right) = \left(\frac{-r}{p}\right) = -\left(\frac{r}{p}\right) = -1$$

ist, so ist auch sie nach der in **3** gebrauchten Schlußweise unmöglich. Wir haben:

Im Falle $m = p \equiv 3 \pmod 4$ kann in $K(\sqrt{m})$ der E. A. nur existieren, wenn alle ganzen Zahlen $\equiv -p+5 \pmod 8$ im Intervall $0, p$ quadratische Nichtreste mod p sind. Ist zuerst $p \equiv 7 \pmod 8$, $p > 7$, so ist $p = 23, 31, 47$ oder $p > 64$. Im letzten Fall existiert ein ganzes rationales A mit $\frac{p+16}{64} < A < \frac{2p+16}{64}$, für das sowohl $8A-2$ als auch $2p-8(8A-2)$ zwischen 0 und p liegen. Beide Zahlen sind $\equiv -p+5 \equiv -2 \pmod 8$, aber eine von ihnen ist quadratischer Rest mod p. — Für $p = 23$ ist 6, für $p = 31$ ist 14, für $p = 47$ ist 6 quadratischer Rest mod p.

Ist zweitens $p \equiv 3 \pmod 8$, $p > 19$, so ist $p = 43$ oder $p = 59$ oder $p > 64$. Im letzteren Falle existiert ein ganzes rationales A mit $\frac{p-8}{32} < A < \frac{p-8}{32} + \frac{p}{64}$, für das sowohl $8A+2$ als auch $8(8A+2)-2p$ zwischen 0 und p liegen. Beide Zahlen sind $\equiv 2 \equiv -p+5 \pmod 8$, aber eine von ihnen ist quadratischer Rest mod p. — Für $p = 43$ ist 10, für $p = 59$ ist 26 quadratischer Rest mod p.

Zusammen mit den sich auf $m = 3, 7, 11$ beziehenden Resultaten von Perron, und indem wir das Resultat der nächsten Nummer schon vorwegnehmen, haben wir damit den

Satz. *Im Falle* $m \equiv 3 \pmod 4$ *existiert in* $K(\sqrt{m})$ *der E. A. nur für* $m = 3, 7, 11, 19$.

5. Es gilt, den E. A. in $K(\sqrt{19})$ nachzuweisen. Dazu müssen wir zeigen, daß die Ungleichung (1) bei $m = 19$ für jedes rationale Zahlenpaar a, b in ganzen rationalen x, y lösbar ist. Offenbar dürfen dabei a und b beide auf das abgeschlossene Intervall $(0, \frac{1}{2})$ beschränkt werden. Unter dieser Beschränkung werden wir dann sogar zeigen, daß schon unter den zehn Zahlenpaaren x_i, y_i $(i = 1, 2, \ldots, 10)$

$i=$	1	2	3	4	5	6	7	8	9	10
$x_i=$	0	−1	3	430	90	−80	−19	−6	7	−2
$y_i=$	0	0	1	99	21	−18	−4	−1	2	0

stets eine Lösung von (1) zu finden ist. Wird x, y statt a, b in (1) gesetzt, so beweisen wir nämlich, daß sämtliche Lösungen in x, y aller zehn Ungleichungen

$$|(x-x_i)^2 - 19(y-y_i)^2| < 1 \qquad (i = 1, 2, \ldots, 10)$$

alle rationalen Zahlenpaare x, y mit $0 \leqq x, y \leqq \frac{1}{2}$ umfassen. Es stellt sich dabei heraus, daß alle rationalen Paare x, y mit $0 \leqq x, y \leqq \frac{1}{2}$ schon dadurch erhalten werden, daß wir für jedes x $(0 \leqq x \leqq \frac{1}{2})$ alle reellen y aus je einer der Ungleichungen

$$0 \leqq y < \alpha_1 \varkappa \sqrt{x^2 + \alpha_1}\,,$$

$$y_i + \alpha_i \varkappa \sqrt{(x - x_i)^2 - \alpha_i} < y < y_i + \alpha_i \varkappa \sqrt{(x - x_i)^2 + \alpha_i} \quad (i = 2, 3, \ldots, 10)$$

bestimmen. Dabei ist $\varkappa = \dfrac{1}{\sqrt{19}}$ und $\alpha_i = 1$ für $x_i \leqq 0$, $\alpha_i = -1$ sonst.

Wir setzen

$$f_{i,\mu}(x) = y_i + \alpha_i \varkappa \sqrt{(x - x_i)^2 + \mu\alpha_i} \quad (i = 1, \mu = 1;\ i = 2, 3, \ldots, 10,\ \mu = \pm 1).$$

Die vorigen Ungleichungen lauten dann

$$0 \leqq y < f_{1,1}(x)\,,$$

$$f_{i,-1}(x) < y < f_{i,1}(x) \qquad (i = 2, 3, \ldots, 10).$$

Offenbar genügt es nun, folgendes zu zeigen: Die Funktionen

$$g_i(x) = f_{i,1}(x) - f_{i+1,-1}(x) \qquad (i = 1, 2, \ldots, 9)$$

$$g_{10}(x) = f_{10,1}(x) - \tfrac{1}{2}$$

sind für $0 \leqq x \leqq \frac{1}{2}$ nicht negativ; für $g_i(x) = 0$ $(i = 1, 2, \ldots, 9)$ ist entweder x oder $f_{i,1}(= f_{i+1,-1}(x))$ irrational; schließlich ist $g_{10}(x) > 0$ für $0 \leqq x \leqq \frac{1}{2}$.

Die letzte Behauptung ist aber wegen

$$g_{10}(x) = \varkappa \sqrt{(x + 2)^2 + 1} - \frac{1}{2} \geqq \frac{\sqrt{5}}{\sqrt{19}} - \frac{1}{2} > 0$$

für $x \geqq 0$ richtig. — Für das übrige beweisen wir den

Hilfssatz. *Die Funktionen* $g_i(x)$ $(i = 1, 2, \ldots, 9)$ *sind im Intervall* $0 \leqq x \leqq \frac{1}{2}$ *monoton zunehmend oder abnehmend, je nachdem* $i = 3, 4$ *ist oder nicht.*

Es ist nämlich

$$g_i'(x) = \frac{dg_i(x)}{dx} = \varkappa\left(\frac{\alpha_i(x - x_i)}{\sqrt{(x - x_i)^2 + \alpha_i}} - \frac{\alpha_{i+1}(x - x_{i+1})}{\sqrt{(x - x_{i+1})^2 - \alpha_{i+1}}}\right)$$

oder

$$g_i'(x) = \varkappa\left(\frac{|x_i| + \alpha_i x}{\sqrt{(|x_i| + \alpha_i x)^2 + \alpha_i}} - \frac{|x_{i+1}| + \alpha_{i+1} x}{\sqrt{(|x_{i+1}| + \alpha_{i+1} x)^2 - \alpha_{i+1}}}\right).$$

Somit ist

$$g_1'(x) = \varkappa\left(\frac{x}{\sqrt{x^2 + 1}} - \frac{1 + x}{\sqrt{(1 + x)^2 - 1}}\right) < 0 \qquad \left(0 < x \leqq \frac{1}{2}\right).$$

Für $i = 2, 3, \ldots, 9$ ist $|x_i| \geqq 1$, so daß beide Brüche in $g_i'(x)$ positiv sind für $0 \leqq x \leqq \frac{1}{2}$. D. h. es ist, wenn $|x_i| + \alpha_i x = u_i$ gesetzt wird,

$$g_i'(x) \gtreqless 0\,,$$

je nachdem

$$\frac{u_i^2}{u_i^2 + \alpha_i} \gtreqless \frac{u_{i+1}^2}{u_{i+1}^2 - \alpha_{i+1}}, \quad \text{d. h.} \quad -\alpha_{i+1} u_i^2 \gtreqless \alpha_i u_{i+1}^2$$

oder

$$-\alpha_{i+1}(|x_i| + \alpha_i x)^2 \gtreqless \alpha_i(|x_{i+1}| + \alpha_{i+1} x)^2$$

ist. Wegen $||x_i| - |x_{i+1}|| \geqq 2$ $(i = 2, 3, \ldots, 9)$ ist Gleichheit für $0 \leqq x \leqq \frac{1}{2}$ aber ausgeschlossen, und x läßt sich einfach streichen:

$$-\alpha_{i+1} x_i^2 \gtrless \alpha_i x_{i+1}^2 ,$$

d. h.

$$-\alpha_{i+1} |x_i| \gtrless \alpha_i |x_{i+1}| .$$

Wegen $\alpha_i = -\dfrac{|x_i|}{x_i}$ $(i = 2, 3, \ldots, 9)$ geht dies in

$$-\frac{1}{x_{i+1}} \gtrless \frac{1}{x_i}$$

über. Hieraus folgt der Hilfssatz.

Auf Grund dieses Hilfssatzes haben wir nur noch zu beweisen, daß

$$g_i(0) > 0 \qquad (i = 3, 4)$$

$$g_i\left(\frac{1}{2}\right) > 0 \qquad (i = 2, 5, 6, 7, 8, 9)$$

$$g_1\left(\frac{1}{2}\right) = 0$$

und $f_{1,1}\left(\frac{1}{2}\right) = f_{2,-1}\left(\frac{1}{2}\right)$ irrational ist.

Die letzten Behauptungen folgen sofort aus $f_{1,1}\left(\frac{1}{2}\right) = f_{2,-1}\left(\frac{1}{2}\right) = \sqrt{\frac{5}{76}}$. Die übrigen Behauptungen lauten für $i = 2, 3, \ldots, 9$ nacheinander:

$$-1 + \varkappa(\sqrt{1{,}5^2 + 1} + \sqrt{2{,}5^2 + 1}) > 0 ,$$
$$-98 + \varkappa(-\sqrt{3^2 - 1} + \sqrt{430^2 + 1}) > 0 ,$$
$$78 + \varkappa(-\sqrt{430^2 - 1} + \sqrt{90^2 + 1}) > 0 ,$$
$$39 + \varkappa(-\sqrt{89{,}5^2 - 1} - \sqrt{80{,}5^2 - 1}) > 0 ,$$
$$-14 + \varkappa(\sqrt{80{,}5^2 + 1} - \sqrt{19{,}5^2 - 1}) > 0 ,$$
$$-3 + \varkappa(\sqrt{19{,}5^2 + 1} - \sqrt{6{,}5^2 - 1}) > 0 ,$$
$$-3 + \varkappa(\sqrt{6{,}5^2 + 1} + \sqrt{6{,}5^2 + 1}) > 0 ,$$
$$2 + \varkappa(-\sqrt{6{,}5^2 - 1} - \sqrt{2{,}5^2 - 1}) > 0 .$$

Sie lassen sich sofort bestätigen, so daß die Existenz des E. A. in $K(\sqrt{19})$ dargetan ist.

6. Jetzt wenden wir uns dem Falle $m \equiv 1 \pmod 4$ zu, in dem dann nach **1** entweder $m = p$ oder $m = pq$ mit $p \equiv q \equiv 3 \pmod 4$ ist.

Es wird im folgenden bequem sein, ein Symbol für den Sachverhalt zu haben, daß bei zwei gegebenen ganzen rationalen Zahlen a, b für jede rationale Primzahl s, die in b in einer ungeraden höchsten Potenz aufgeht, das Kroneckersche Symbol $\left(\frac{a}{s}\right) = 1$ ist, daß also, mit anderen Worten, für die Darstellung $b = b_1 b_2 \cdots$ von b als ein Produkt von relativ primen Primzahlpotenzen, die Gleichungen $\left(\frac{a}{b_1}\right) = \left(\frac{a}{b_2}\right) = \cdots = 1$ bestehen. Wir wollen das kurz durch

$$\left(\frac{a}{b}\right)^* = 1$$

wiedergeben.

Wir beweisen den

Satz. *Existiert in* $K(\sqrt{m})$ *mit* $m \equiv 1 \pmod 4$ *der E. A., so gilt:*

1. *Für jede ganze rationale Zahl* r *mit*

$$\left(\frac{r}{m}\right)^* = 1 \qquad (0 < r < m;\ (r, m) = 1)$$

ist entweder

$$\left(\frac{m}{r}\right)^* = 1$$

oder

$$\left(\frac{m}{r-m}\right)^* = 1.$$

2. *Im Falle eines zusammengesetzten* m, *wo man dann* $m = pq$ *mit* $p \equiv q \equiv 3 \pmod 4$ *annehmen darf, ist für jede ganze rationale Zahl* r *mit*

$$\left(\frac{r}{p}\right) = \left(\frac{q}{p}\right) \qquad (0 < r < p;\ (r, q) = (r - p, q) = 1)$$

entweder

$$\left(\frac{m}{r}\right)^* = 1, \text{ gleichzeitig also auch } \left(\frac{r}{q}\right) = \left(\frac{q}{p}\right),$$

oder

$$\left(\frac{m}{r-p}\right)^* = 1, \text{ gleichzeitig also auch } \left(\frac{r-p}{q}\right) = \left(\frac{q}{p}\right).$$

Beweis. Wir stützen uns auf den Hilfssatz aus **2**. Wird für jedes ganze rationale $r \neq 0$ die ungerade ganze rationale Zahl r_0 durch $r = 2^e r_0$ mit ganzem rationalen e definiert und bestehen für r die Voraussetzungen von Teil 1, so folgt aus dem genannten Hilfssatz, daß entweder

$$\left(\frac{m}{r_0}\right)^* = 1 \quad \text{oder} \quad \left(\frac{m}{(r-m)_0}\right)^* = 1$$

ist. Im ersten Falle folgt $\left(\frac{m}{r_0}\right) = 1$ und dabei wegen $\left(\frac{r}{m}\right)^* = 1$ auch $\left(\frac{m}{r}\right) = \left(\frac{r}{m}\right) = 1$, woraus auf $\left(\frac{m}{2^e}\right) = 1$ zu schließen ist mit $r = 2^e r_0$. Im zweiten Falle kann man ähnlich schließen, da dann $\left(\frac{m}{(r-m)_0}\right) = 1$, wegen $\left(\frac{r}{m}\right)^* = 1$ auch $\left(\frac{m}{r-m}\right) = \left(\frac{r-m}{m}\right) = \left(\frac{r}{m}\right) = 1$, also wieder $\left(\frac{m}{2^e}\right) = 1$, wobei jetzt $r - m = 2^e (r-m)_0$. Damit ist Teil 1 des Satzes bewiesen.

Bestehen für r die Voraussetzungen von Teil 2, so ist (3) für qr (statt r) lösbar und $0 < qr < m$. Somit können wir den Hilfssatz in **2** auf qr statt auf r anwenden. Dann aber muß y_1 in (2″) durch q teilbar sein, und somit ist in ganzen rationalen x, y_2

$$px^2 - qy_2^2 = -4r \text{ oder } = 4(p-r) \qquad (x \equiv y_2 \pmod 2).$$

Daraus folgt wieder

$$\left(\frac{pq}{r_0}\right)^* = 1 \quad \text{bzw.} \quad \left(\frac{pq}{(r-p)_0}\right)^* = 1.$$

Man schließt nun ähnlich weiter wie früher, da

$$\left(\frac{pq}{r}\right) = \left(\frac{r}{pq}\right) = \left(\frac{r}{p}\right)\left(\frac{r}{q}\right) = \left(\frac{q}{p}\right)\left(\frac{r}{q}\right) = \left(\frac{q}{p}\right)\left(\frac{-p}{q}\right) = 1$$

bzw.

$$\left(\frac{pq}{r-p}\right)=\left(\frac{r-p}{pq}\right)=\left(\frac{r-p}{p}\right)\left(\frac{r-p}{q}\right)=\left(\frac{r}{p}\right)\left(\frac{r-p}{q}\right)=\left(\frac{q}{p}\right)\left(\frac{r-p}{q}\right)=\left(\frac{q}{p}\right)\left(\frac{-p}{q}\right)=1.$$

Damit ist auch Teil 2 des Satzes bewiesen.

7. Aus Teil 2 des letzten Satzes ziehen wir für den Fall, daß in $K(\sqrt{m})$ der E. A. vorhanden ist und daß $m = pq$ mit $p \equiv q \equiv 3 \pmod 4$ gilt, eine später zu benützende Folgerung.

Es gebe nämlich ein ganzes rationales a mit $2 \leqq a \leqq q-1$ so, daß

$$\left(\frac{a}{q}\right)=\left(\frac{a-1}{q}\right)=1$$

ist. Dann ist

$$\left(\frac{pa}{q}\right)=\left(\frac{p(a-1)}{q}\right)=\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right).$$

Es gebe ferner ein ganzes rationales r mit $r \equiv pa \pmod q$, $0 < r < p$, wobei dann natürlich $(r, q) = 1$ und $(r-p, q) = (p(a-1), q) = 1$ ist. Da nach Obigem

$$\left(\frac{r}{q}\right)=\left(\frac{r-p}{q}\right)=-\left(\frac{q}{p}\right)$$

ist, so folgt aus Teil 2 des vorigen Satzes:

$$\left(\frac{r}{p}\right)=-\left(\frac{q}{p}\right).$$

Somit sind alle ganzen rationalen Zahlen im Innern des Intervalls $0, p$, die $\equiv pa \pmod q$ sind, von entgegengesetztem quadratischen Charakter mod p wie q. Subtrahiert man pa von allen diesen Zahlen, so erkennt man, daß alle durch q teilbaren ganzen rationalen Zahlen im Innern des Intervalls $-pa, -p(a-1)$ ebenfalls von entgegengesetztem quadratischen Charakter mod p sind wie q. Teilt man alle diese Zahlen durch q, so folgt also, daß die ganzen rationalen Zahlen im Intervall $-\frac{p}{q}a, -\frac{p}{q}(a-1)$ quadratische Nichtreste mod p, d. h. die ganzen rationalen Zahlen des Intervalls $\frac{p}{q}(a-1), \frac{p}{q}a$ quadratische Reste mod p sind.

Daraus ergibt sich gleich allgemeiner: Sind x, y $(0 < x < y < p)$ ganze rationale Zahlen derart, daß die ganzen rationalen Zahlen des Intervalls x, y aus lauter quadratischen Resten mod q bestehen, so sind alle ganzen rationalen Zahlen des Intervalls $\frac{p}{q}x, \frac{p}{q}y$ quadratische Reste mod p.

Wir nennen die Zahlen $x, x+1, \ldots, y$ eine Sequenz für q, wenn außer

$$\left(\frac{x}{q}\right)=\left(\frac{x+1}{q}\right)=\cdots=\left(\frac{y}{q}\right)=1$$

noch $\left(\frac{x-1}{q}\right)=\left(\frac{y+1}{q}\right)\neq 1$ gilt. Die Anzahl der Glieder dieser Sequenz ist $y-x+1$ $(\geqq 2)$. Ordnen wir dieser Sequenz das Intervall $i = x, y$ zu und bezeichnen wir das Intervall cx, cy $(c > 0)$ einfach mit ci, so sieht man nach Vertauschung von p und q:

Sind unter den eingangs über m gemachten Voraussetzungen $i, k, l, \ldots$ die allen Sequenzen für p zugeordneten Intervalle, so sind die Intervalle $\frac{q}{p}i, \frac{q}{p}k, \frac{q}{p}l, \ldots$ paarweise

ohne gemeinsame Punkte, und alle in ihnen gelegenen ganzen rationalen Zahlen sind quadratische Reste mod q.

8. Mit Hilfe dieser Tatsache beweisen wir nun den

Satz. *In $K(\sqrt{m})$ gelte der E. A. Es sei $m \equiv 1 \pmod 4$, $m = pq$, $p \equiv q \equiv 3 \pmod 4$, $p < q$. Dann ist*

$$q \leqq 3p + 17 + \frac{101}{p-6} \quad \textit{für} \quad p \geqq 7$$

und sogar

$$q < 2p \quad \textit{für} \quad p > 2500.$$

Beweis. Es bezeichne $p(a_1, a_2, \ldots, a_e)$ die Anzahl der Lösungen von

$$\left(\frac{r}{p}\right) = a_1, \left(\frac{r+1}{p}\right) = a_2, \ldots, \left(\frac{r+e-1}{p}\right) = a_e, \; 0 < r < p,$$

unter $a_1, a_2, \ldots, a_e$ irgendein System von Zahlen ± 1 verstanden. Dann ist nach Lagrange

$$p(1,1) = \left[\frac{p}{4}\right], \tag{4}$$

nach Jacobsthal [10])

$$p(1,1,1) = \left[\frac{p}{8}\right] \tag{5}$$

und nach Hasse [11])

$$\left| p(a_1, a_2, a_3, a_4) - \frac{p}{16} \right| < \frac{6\sqrt{p} + 22}{16}. \tag{6}$$

Bezeichnet noch $p_e (e \geqq 2)$ die Anzahl der e-gliedrigen Sequenzen für p im obigen Sinne, so kann man (4) offenbar in der Gestalt

$$\sum_{e \geqq 2} p_e(e-1) = \left[\frac{p}{4}\right] \tag{7}$$

schreiben. Ähnlich folgt aus (5)

$$\sum_{e \geqq 2} p_e(e-2) = \left[\frac{p}{8}\right]. \tag{8}$$

Weiter ist $p(-1,1,1,-1) = p_2 - 1$ oder $= p_2$, je nachdem nämlich die Anfangswerte der Folge $\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \left(\frac{3}{p}\right), \ldots$ die Zahlen $1, 1, -1$ sind oder nicht. Jedenfalls ist also nach (6)

$$\frac{p - 6\sqrt{p} - 22}{16} < p_2 < \frac{p + 6\sqrt{p} + 38}{16}. \tag{9}$$

Aus (7) und (8) folgt sofort

$$\sum_{e \geqq 2} p_e = \left[\frac{p}{4}\right] - \left[\frac{p}{8}\right], \tag{10}$$

$$\sum_{e \geqq 2} e p_e = 2\left[\frac{p}{4}\right] - \left[\frac{p}{8}\right] \tag{11}$$

[10]) E. Jacobsthal, Anwendungen einer Formel aus der Theorie der quadratischen Reste, Dissertation Berlin 1906, S. 29.

[11]) H. Hasse, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abh. Math. Sem. Hamburg **10** (1934), S. 325—348, insbesondere S. 347.

und hieraus

$$2p_2 + 3p_3 + 4p_4 + 5\sum_{e\geqq 5} p_e \leqq 2\left[\frac{p}{4}\right] - \left[\frac{p}{8}\right],$$

$$5\sum_{e\geqq 2} p_e - 3p_2 - 2p_3 - p_4 \leqq 2\left[\frac{p}{4}\right] - \left[\frac{p}{8}\right].$$

Daraus ergibt sich nach (10)

$$2p_3 + p_4 \geqq 3\left[\frac{p}{4}\right] - 4\left[\frac{p}{8}\right] - 3p_2. \tag{12}$$

Ist nun i ein Intervall der Länge $\bar{i}$, das einer Sequenz (aus $\bar{i}+1$ Gliedern) für p zugeordnet ist, so enthält das Intervall $\frac{q}{p}\,i$ wenigstens $\left[\frac{q}{p}\,\bar{i}\right]$ ganze rationale Zahlen. Da alle diese nach Obigem quadratische Reste mod q sind, gibt es darunter wenigstens $\left[\frac{q}{p}\,\bar{i}\right] - 2$ solche Zahlen r, für welche $\left(\frac{r}{q}\right) = \left(\frac{r+1}{q}\right) = \left(\frac{r+2}{q}\right) = 1$ ist. (Natürlich hat diese Aussage nur einen Sinn, wenn $\left[\frac{q}{p}\,\bar{i}\right] - 2 > 0$ ist.) Offenbar ist also

$$\sum_{e\geqq 2} p_e\left(\left[\frac{q}{p}\,(e-1)\right] - 2\right) \leqq q(1,1,1). \tag{13}$$

(Die Anzahlfunktionen $q(a_1, a_2, \ldots, a_e)$ bzw. q_e sind für q analog definiert, wie das oben für p geschah.) Genau so folgt

$$\sum_{e\geqq 2} p_e\left(\left[\frac{q}{p}\,(e-1)\right] - 3\right) \leqq q(1,1,1,1). \tag{14}$$

Nach Konstruktion bleiben diese Ungleichungen auch dann richtig, wenn die Summation nur über $e \geqq 3$ erstreckt wird. Dies bedeutet eventuell eine Verschärfung durch Weglassen negativer Glieder.

Es sei von nun an $7 \leqq p < q$. Wir wollen $\frac{q}{p}$ auf Grund von (13) nach oben abschätzen. Später wird diese Abschätzung dann durch zweimalige Anwendung von (14) verfeinert werden.

Wegen

$$\left[\frac{q}{p}\,(e-1)\right] \geqq \frac{q}{p}\,(e-1) - 1 + \frac{1}{p} \tag{15}$$

können wir (13) in

$$\sum_{e\geqq 2} p_e\left(\frac{q}{p}\,e - 3 - \frac{q-1}{p}\right) \leqq q(1,1,1)$$

umwandeln. Aus (5), (10) und (11) folgt dann

$$\frac{q}{p}\left(2\left[\frac{p}{4}\right] - \left[\frac{p}{8}\right]\right) - \left(3 + \frac{q-1}{p}\right)\left(\left[\frac{p}{4}\right] - \left[\frac{p}{8}\right]\right) \leqq \left[\frac{q}{8}\right],$$

d. h. nach Multiplikation mit p

$$(q - 3p + 1)\left[\frac{p}{4}\right] + (3p - 1)\left[\frac{p}{8}\right] \leqq p\left[\frac{q}{8}\right].$$

Es ist $\left[\frac{p}{4}\right] = \frac{p-3}{4}$, $\left[\frac{p}{8}\right] \geqq \frac{p-7}{8}$, $\left[\frac{q}{8}\right] \leqq \frac{q-3}{8}$ und somit

$$2(q - 3p + 1)(p - 3) + (3p - 1)(p - 7) \leqq p(q - 3),$$

d. h.

$$(p-6)\,q \leqq 3p^2 - p - 1\,.$$

Somit ist

$$q \leqq \frac{3p^2 - p - 1}{p-6} = 3p + 17 + \frac{101}{p-6} \tag{16}$$

und daher jedenfalls für $p \geqq 23$

$$q < 3p + 17 + \frac{101}{17} < 3p + 23 \leqq 4p\,.$$

Über die vorige Annahme $p \geqq 7$ hinaus nehmen wir jetzt $q < 4p$ an. Wie schon bemerkt war, können wir in (14) von dem Wert $e = 2$ absehen. Mittels (15) erhalten wir dann aus (14)

$$\sum_{e \geqq 3} p_e \left(\frac{q}{p}\, e - 4 - \frac{q-1}{p} \right) \leqq q(1, 1, 1, 1),$$

d. h.

$$\sum_{e \geqq 2} p_e \left(\frac{q}{p}\, e - 4 - \frac{q-1}{p} \right) + p_2 \left(4 - \frac{q+1}{p} \right) \leqq q(1, 1, 1, 1)\,.$$

Wegen $q < 4p$ ist $4 - \frac{q+1}{p} \geqq 0$, sodaß wir im zweiten Glied links p_2 nach (9) durch $\frac{p - 6\sqrt{p} - 22}{16}$ ersetzen können. Wenden wir dann noch (6), (10) und (11) an, so erhalten wir

$$\frac{q}{p}\left(2\left[\frac{p}{4}\right] - \left[\frac{p}{8}\right]\right) - \left(4 + \frac{q-1}{p}\right)\left(\left[\frac{p}{4}\right] - \left[\frac{p}{8}\right]\right) + \frac{p - 6\sqrt{p} - 22}{16}\left(4 - \frac{q+1}{p}\right)$$

$$< \frac{q + 6\sqrt{q} + 22}{16}\,.$$

Hieraus folgt nach Ersetzen der eckigen Klammern durch ihre Werte wie oben

$$q < \frac{4p^2 + 24p\sqrt{p} + 117p - 6\sqrt{p} - 24 + 6p\sqrt{q}}{2p + 6\sqrt{p} + 10}$$

und also wegen $\sqrt{q} < 2\sqrt{p}$

$$q < 2p + \frac{24p\sqrt{p} + 97p - 6\sqrt{p} - 24}{2p + 6\sqrt{p} + 10} = 2p + 12\sqrt{p} + \frac{25p - 126\sqrt{p} - 24}{2p + 6\sqrt{p} + 10}$$

und somit schließlich

$$q < 2p + 12\sqrt{p} + \frac{25}{2} - \frac{201\sqrt{p} + 149}{2p + 6\sqrt{p} + 10} < 2p + 12\sqrt{p} + \frac{25}{2}\,.$$

Insbesondere ist daher für $p > 2500$

$$q < 2p + \frac{p}{4}\,.$$

Über die früheren Annahmen hinaus nehmen wir jetzt $2p < q < 2p + \frac{p}{4}$ an. Dann folgt wegen $2 < \frac{q}{p}$ aus (14), wobei wir wieder $e = 2$ in der Summe weglassen:

$$\sum_{e \geqq 5} p_e \left(\left[\frac{q}{p}\,(e-1) \right] - 3 \right) + p_3 + 3p_4 \leqq q(1, 1, 1, 1)\,,$$

und daraus nach (15)

$$\sum_{e\geqq 5} p_e\left(\frac{q}{p}e-4-\frac{q-1}{p}\right)+p_3+3p_4\leqq q(1,1,1,1)\,.$$

Es ist also

$$\sum_{e\geqq 2} p_e\left(\frac{q}{p}e-4-\frac{q-1}{p}\right)+p_2\left(4-\frac{q+1}{p}\right)+p_3\left(5-\frac{2q+1}{p}\right)+p_4\left(7-\frac{3q+1}{p}\right)\leqq q(1,1,1,1)\,.$$

Hier ist die Summe aus den zwei letzten Gliedern links gleich

$$\frac{1}{2}(2p_3+p_4)\left(5-\frac{2q+1}{p}\right)+p_4\left(\frac{9}{2}-\frac{4q+1}{2p}\right).$$

Wegen $\frac{q}{p}<2+\frac{1}{4}$ ist dabei $\frac{9}{2}-\frac{4q+1}{2p}=\frac{9p-4q-1}{2p}\geqq 0$. Daher folgt wegen (12)

$$\sum_{e\geqq 2} p_e\left(\frac{q}{p}e-4-\frac{q-1}{p}\right)+p_2\left(4-\frac{q+1}{p}\right)+\frac{1}{2}\left(3\left[\frac{p}{4}\right]-4\left[\frac{p}{8}\right]-3p_2\right)\left(5-\frac{2q+1}{p}\right)\leqq q(1,1,1,1)\,.$$

Summiert man hierbei wie oben, so erhält man

$$\frac{q}{p}\left(2\left[\frac{p}{4}\right]-\left[\frac{p}{8}\right]\right)-\left(4+\frac{q-1}{p}\right)\left(\left[\frac{p}{4}\right]-\left[\frac{p}{8}\right]\right)+\left(\frac{5}{2}-\frac{2q+1}{2p}\right)\left(3\left[\frac{p}{4}\right]-4\left[\frac{p}{8}\right]\right)+p_2\left(-\frac{7}{2}+\frac{4q+1}{2p}\right)\leqq q(1,1,1,1)$$

oder nach Multiplikation mit $2p$

$$(-4q+7p-1)\left[\frac{p}{4}\right]+(8q-12p+2)\left[\frac{p}{8}\right]+p_2(4q-7p+1)\leqq 2p\cdot q(1,1,1,1)\,.$$

Der Koeffizient von p_2 ist hierbei positiv, sodaß wir p_2 nach (9) durch $\frac{p-6\sqrt{p}-22}{16}$ ersetzen können. Multiplizieren wir überdies noch mit 16 und ersetzen wir die eckigen Klammern wie oben, so kommt

$$(-4q+7p-1)(4p-12)+(8q-12p+2)(2p-14)+(4q-7p+1)(p-6\sqrt{p}-22)\leqq 2p(q+6\sqrt{q}+22)\,.$$

Da nunmehr $\sqrt{q}<\frac{3}{2}\sqrt{p}$ ist, ergibt sich

$$(-4q+7p-1)(3p+6\sqrt{p}+10)+(8q-12p+2)(2p-14)<2p(q+9\sqrt{p}+22)\,.$$

Es ist also

$$q<\frac{3p^2-24p\sqrt{p}-195p+6\sqrt{p}+38}{2p-24\sqrt{p}-152}=\frac{3p}{2}+\frac{12p\sqrt{p}+33p+6\sqrt{p}+38}{2p-24\sqrt{p}-152}$$
$$=\frac{3p}{2}+6\sqrt{p}+\frac{177p+918\sqrt{p}+38}{2p-24\sqrt{p}-152}\,.$$

Hieraus folgt aber wegen $p>2500$ der Widerspruch

$$\frac{q}{p}<\frac{3}{2}+\frac{6}{\sqrt{p}}+\frac{1}{p}\,\frac{177p+20p}{2p-p}<\frac{3}{2}+\frac{6}{50}+\frac{197}{2500}<\frac{3}{2}+\frac{1}{8}+\frac{1}{10}<2\,.$$

Die Annahme $\frac{q}{p}>2$ war falsch für $p>2500$, und der Satz ist bewiesen.

9. Wir beweisen den

Satz. *In der Restklasse* $m \equiv 5 \pmod 8$ *gibt es keine zusammengesetzten Zahlen derart, daß im Körper* $K(\sqrt{m})$ *der E. A. gilt, ausgenommen den Fall* $m = 3p$, $p \equiv 3 \pmod 4$.

Beweis. In $K(\sqrt{m})$ gelte der E. A. und es sei $m = pq$, $p \equiv q \equiv 3 \pmod 4$, $3 < p < q$. Ist $p \geqq 11$, so gibt es nach (5) ein r mit $0 < r < p$ und $\left(\frac{r}{p}\right) = \left(\frac{r+1}{p}\right) = \left(\frac{r+2}{p}\right)$. Wir können $r = 2s$ annehmen, s ganz, da im Falle $2 \nmid r$ man r durch $p - r - 2$ ersetzen kann und hier ebenfalls $\left(\frac{p-r-2}{p}\right) = \left(\frac{p-r-1}{p}\right) = \left(\frac{p-r}{p}\right)$ gilt. Offenbar ist dann auch $\left(\frac{s}{p}\right) = \left(\frac{s+1}{p}\right)$. Wegen $p < q$ liegt eine ganze rationale Zahl t zwischen $\frac{q}{p}s$ und $\frac{q}{p}(s+1)$. Dann ist $\left(\frac{s}{p}\right) = \left(\frac{t}{q}\right)$. Ist nämlich $\left(\frac{s}{p}\right) = 1$, so folgt die Behauptung $\left(\frac{t}{p}\right) = 1$ aus **7**. Ist aber $\left(\frac{s}{p}\right) = -1$, so ist $\left(\frac{p-s-1}{p}\right) = \left(\frac{p-s}{p}\right) = 1$. Nun liegt aber $q - t$ zwischen $\frac{q}{p}(p-s-1)$ und $\frac{q}{p}(p-s)$, sodaß $\left(\frac{q-t}{q}\right) = 1$, d. h. $\left(\frac{t}{q}\right) = -1 = \left(\frac{s}{p}\right)$ auch in diesem Falle folgt.

Da auch $\left(\frac{2s}{p}\right) = \left(\frac{2s+1}{p}\right) = \left(\frac{2s+2}{p}\right)$ ist und $2t$ zwischen $\frac{q}{p}2s$ und $\frac{q}{p}(2s+2)$ liegt, schließt man genau so, daß $\left(\frac{2s}{p}\right) = \left(\frac{2t}{q}\right)$ ist. Zusammen mit dem Vorhergehenden ergibt dies $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$, d. h. $m = pq \equiv 1 \pmod 8$.

Zum vollständigen Beweis des Satzes ist also nur noch der Fall $p = 7$ zu prüfen. Für $p = 7$ ist dann nach dem vorigen Abschnitt $q \leqq 3 \cdot 7 + 17 + 101 = 139$. Wegen $q \equiv 3 \pmod 4$ sind daher nur noch die Primzahlen 11, 19, 43, 59, 67, 83, 107, 131 und 139 zu betrachten. Nun ist aber $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = 1$. Nach **7** scheiden diese Primzahlen also alle aus, da für jede von ihnen im Intervall $\frac{q}{7}, \frac{2q}{7}$ eine ganze rationale Zahl n mit $\left(\frac{n}{q}\right) = -1$ existiert. Wir geben in Klammern beigefügt zu jedem der fraglichen q ein solches n an: 11 (2), 19 (3), 43 (8), 59 (10), 67 (8), 83 (15), 107 (18), 131 (24), 139 (32). Damit ist der Satz bewiesen.

10. Wir beweisen zum Schluß noch den

Satz. *In* $K(\sqrt{m})$ *mit* $m \equiv 5 \pmod{24}$ *existiert der E. A. nur für* $m = 5$ *oder* $m = 29$.

Beweis. Nach dem vorigen Satz ist nur noch $m = p$ zu betrachten. Es sei daher $m = p \equiv 5 \pmod{24}$ und in $K(\sqrt{p})$ der E. A. vorhanden. Wir wählen eine ganze rationale Zahl s mit $0 < s < \frac{p}{3}$, $(s, 3p) = 1$, $s \equiv 1 \pmod 4$. Für sie ist $3s - p \equiv 2 \pmod 4$, sodaß wegen $\left(\frac{p}{2}\right) = -1$ die Beziehung $\left(\frac{p}{3s-p}\right)^* = 1$ nicht besteht; ebenso besteht $\left(\frac{p}{3s}\right)^* = 1$ nicht wegen $\left(\frac{p}{3}\right) = -1$. Nach dem Teil 1 des Satzes in **6**, angewandt auf $r = 3s$, folgt daher, daß $\left(\frac{3s}{p}\right)^* = 1$ nicht besteht. Stets ist also $\left(\frac{3s}{p}\right) = -1$, d. h. $\left(\frac{s}{p}\right) = 1$. Hieraus

folgt aber sofort $p < 432$. Denn andernfalls existierte ein ganzes rationales A mit

$$\frac{2p-36}{432} < A < \frac{2p-36}{432} + \frac{p}{432}.$$

Wir setzen $s_1 = 12A + 1$, $s_2 = p - 144A - 12$. Dann ist $0 < s_1, s_2 < \frac{p}{3}$; $3 \nmid s_1, s_2$; $s_1, s_2 \equiv 1 \pmod 4$. Beide Zahlen s_1, s_2 sind demnach als Zahlen s zu betrachten, und doch ist wegen $s_2 = p - 12s_1$ und $\left(\frac{3}{p}\right) = -1$:

$$\left(\frac{s_2}{p}\right) = -\left(\frac{s_1}{p}\right).$$

Es bleiben also nur noch die Primzahlen $p = 5, 29, 101, 149, 269, 389$ übrig. Davon fallen die vier letzten wegen $\left(\frac{29}{101}\right) = \left(\frac{13}{149}\right) = \left(\frac{29}{269}\right) = \left(\frac{29}{389}\right) = -1$ weg. Für $p = 5$ und $p = 29$ existiert jedoch nach dem in der Einleitung Gesagten der E. A. wirklich. Der Satz ist also bewiesen.

Zusatz bei der Korrektur. Inzwischen hat Hofreiter in der Arbeit „Quadratische Körper mit und ohne Euklidischen Algorithmus“, Monatsh. f. Math. u. Phys. **42** (1935), S. 397—400 bewiesen, daß der E. A. für $m \equiv 21 \pmod{24}$, $m > 21$, d. h. für $3|m$, $m \equiv 5 \pmod 8$, $m > 21$, desgleichen für $m = 77$ nicht, dagegen für $m = 57$ gilt. Somit gilt unser Satz in **9** mit der alleinigen Ausnahme $m = 21$. Dabei ist der Fall $m = 77 = 7 \cdot 11 \equiv 5 \pmod 8$ in eben diesem Satz schon inbegriffen.

Die Hofreitersche Arbeit enthält einige Fehler, die jedoch das Resultat nicht beeinflussen. So ist z. B. auf S. 398 Z. 15 „$8q^2 - 4d$“ statt „$4d - 8q^2$“ zu lesen.

Eingegangen 6. Juni 1935.

Funktionen, die den Potenzen der Riemannschen Zetafunktion verwandt sind, und Potenzreihen, die über den Einheitskreis nicht fortsetzbar sind.

Von *H. Kober* in Breslau.

Über $\sum_{n \leqq \omega} d(n) \cos 2\pi n v$ und verwandte Summen[1]) sind eine Reihe von Ergebnissen von Chowla und Walfisz bewiesen worden, wobei v, bis auf einen Fall, irrational ist. Herr Wilton hat, wieder mit anderem Beweisverfahren, noch einige Ergebnisse hinzugefügt, darunter auch solche für rationales v.

Während nun über die Funktionen

$$Z_{\frac{1}{2}}(s; v; 0) = \sum_{n=1}^{\infty} \frac{d(n)}{n^s} \cdot \begin{cases} \cos 2\pi v n \\ \sin 2\pi v n \end{cases}, \qquad \text{allgemeiner} \qquad Z_{\frac{1}{2}}(s; v; w) = \sum_{n=1}^{\infty} \frac{\sigma_{2w}(n)}{n^{s+w}} \cdot \begin{cases} \cos 2\pi v n \\ \sin 2\pi v n \end{cases}$$

für irrationale Werte von v nichts weiter bekannt ist, als was sich durch allgemeine Reihensätze aus diesen Ergebnissen folgern läßt, besitzen diese Funktionen im Falle eines rationalen v sehr einfache, leicht direkt beweisbare analytische Eigenschaften[2]). Es liegt nun nahe, die entsprechend mit $d_h(n)$, der Anzahl der Zerlegungen von n in h Faktoren, gebildeten Reihen zu betrachten; man erhält:

Es seien α und k ganz, $k > 0$, $h > 1$, $s = \sigma + it$, ferner sei für $\sigma > 1$

$$f_0(s; h; k, \alpha) = \sum_{\substack{n \equiv \alpha \,(\mathrm{mod}.\, k) \\ n \neq 0}} d_h(|n|)\, |n|^{-s}, \tag{4a}$$

$$f_1(s; h; k, \alpha) = \sum_{\substack{n \equiv \alpha \,(\mathrm{mod}.\, k) \\ n \neq 0}} d_h(|n|) n\, |n|^{-s-1}, \tag{4b}$$

wobei n alle positiven und negativen Zahlen der arithmetischen Reihe durchläuft. Dann sind

$$(s-1)^h f_0(s) \text{ und } f_1(s)$$

ganze Funktionen, und es gilt für $\mathfrak{a} = 0$ und $\mathfrak{a} = 1$, wenn $\varphi_{\mathfrak{a}}(s)$ eine Funktion bedeutet, die für $\sigma > 1$ durch eine absolut konvergente Dirichletsche Reihe darstellbar ist (vgl. auch Fußnote 8), die Funktionalgleichung

$$f_{\mathfrak{a}}(s)\, \Gamma^h\left(\frac{s+\mathfrak{a}}{2}\right) \left(\frac{\pi}{k}\right)^{-\frac{sh}{2}} = \varphi_{\mathfrak{a}}(1-s)\, \Gamma^h\left(\frac{1+\mathfrak{a}-s}{2}\right) \left(\frac{\pi}{k}\right)^{\frac{s-1}{2}h}. \tag{4c}$$

[1]) Chowla, Some problems of diophantine approximation I, Math. Zeitschr. **33** (1931), S. 544—563. — Walfisz, Über einige trigonometrische Summen, Math. Zeitschr. **33** (1931), S. 564—601. — Wilton, An approximate functional equation ..., dieses Journal **169** (1933), S. 219—237.

[2]) H. Kober, Transformationen einer bestimmten Besselschen Reihe ..., dieses Journal **173** (1935), S. 65—78.

Es sei $v = \frac{a}{c}$ rational, $(a, c) = 1$, dann gelten dieselben Ergebnisse für die allgemeineren Funktionen

$$(4,6) \qquad \sum_{\substack{n \equiv \alpha \,(\mathrm{mod.}\, k) \\ n \neq 0}} d_h(|n|)\, |n|^{-s}\, e^{2i\pi v n}, \qquad \sum_{\substack{n \equiv \alpha \,(\mathrm{mod.}\, k) \\ n \neq 0}} d_h(|n|)\, n\, |n|^{-s-1}\, e^{2i\pi v n},$$

nur tritt in der Funktionalgleichung (4c) an die Stelle von k das kleinste gemeinschaftliche Vielfache von c und k. Entsprechende allgemeinere Ergebnisse erhält man, wenn man statt mit $d_h(n)$ mit der allgemeineren Teilerfunktion

$$\sigma(n; h; w) = \sigma(n; w_1, w_2, \ldots, w_h) = \sum_{\delta_1 \delta_2 \delta_3 \cdots \delta_h = n} \delta_1^{w_1} \delta_2^{w_2} \delta_3^{w_3} \cdots \delta_h^{w_h};\ n, \delta \text{ ganz } > 0$$

arbeitet, die eine Funktion der $h + 1$ Variablen $n, w_1, \ldots, w_h$ ist. Setzt man $d_1(n) = 1$, $\sigma(n; w_1) = n^{w_1}$, so kann man auch den Fall $h = 1$ in die Ergebnisse mit einschließen.

Durch bekannte Sätze über Dirichletsche Reihen werden aus den analytischen Eigenschaften der Funktionen (4, 6) Ergebnisse über die endlichen Summen

$$\sum_{n=1}^{x} d_h(n) \cdot \begin{cases} \cos 2\pi nv \\ \sin 2\pi nv \end{cases}, \qquad h \geqq 2$$

bei rationalem v und über allgemeinere Summen dieser Art gewonnen, die im Falle $h = 2$ bereits bekannt sind.

In der Laurentschen Reihe für $f_0(s)$ im Punkte $s = 1$ möge der Koeffizient von $(s-1)^{-h}$ als *Hauptkoeffizient* bezeichnet werden; die Bestimmung dieses Koeffizienten ist an und für sich von Belang, sie ist auch für die weiteren Anwendungen notwendig; sie erfolgt hier mit Hilfe einer Reihe elementar-zahlentheoretischer Überlegungen (5. Abschnitt).

Von diesen Ergebnissen aus ist es nun möglich, die Nichtfortsetzbarkeit gewisser Potenzreihen über den Einheitskreis hinaus zu beweisen, und zwar auch solcher, bei denen man mit den Kriterien von Herrn Franel[3]) und Herrn Knopp[3]) nicht weiterkommt. Herr Franel hatte bewiesen: Es sei die Lambertsche Reihe

$$F(x) = \sum_{n=1}^{\infty} \frac{b_n x^n}{1 - x^n} = \sum_{m=1}^{\infty} a_m x^m, \qquad \text{also} \quad a_m = \sum_{d|m} b_d,$$

gegeben. x_0 sei eine primitive k-te Einheitswurzel, jede der k Reihen

$$\sum_{n=1}^{\infty} \frac{b_{kn+l}}{kn + l}, \qquad l = 0, 1, \ldots, k-1$$

konvergiere (daher auch die Lambertsche Reihe im Einheitskreise). Dann ist bei radialer Annäherung aus dem Inneren des Kreises für $x \to x_0$

$$\lim \left(1 - \frac{x}{x_0}\right) F(x) = \sum_{\nu=1}^{\infty} \frac{b_{k\nu}}{k\nu}.$$

Fügt man also den Voraussetzungen dieses Satzes (die hier bereits in der von Knopp vorgenommenen Vereinfachung angegeben sind) noch die weitere hinzu: $\sum \frac{b_{k\nu}}{k\nu} \neq 0$, so folgt, daß x_0 ein singulärer Punkt von $F(x)$ ist. Das ist das Franelsche Kriterium.

Herr Knopp zeigte: Eine im Einheitskreis konvergente Lambertsche Reihe mit positiven Koeffizienten b_n stellt eine über den Kreis hinaus nicht fortsetzbare Funktion

---

[3]) Franel, Sur la théorie des séries, Math. Ann. **52** (1899), S. 529—549. — Knopp, Über Lambertsche Reihen, dieses Journal **142** (1913), S. 283—315.

dar, wenn für unendlich viele k

$$\lim_{n=\infty} \frac{\sum_{\nu=1}^{n} b_\nu}{n \sum_{k\nu \leq n} \frac{b_{k\nu}}{k\nu}} = 0$$

ist. Dieses Kriterium erfaßt z. B. auch den Fall $b_n = 1$, $a_n = d(n)$, in dem das Franelsche versagt.

Ist u beliebig komplex, $\sigma_u(n) = \sum_{d|n} d^u$, also in der oben gewählten Bezeichnung $\sigma_u(n) = \sigma(n; u, 0)$, so hat Herr Knopp gezeigt, daß die Reihe $\Sigma \sigma_u(n) x^n$ über den Einheitskreis hinaus nicht fortsetzbar ist; der Fall eines rein imaginären u ist dort nicht behandelt, er wird hier — im Rahmen der Erledigung des allgemeinen Falles auf neuem Wege — mit bewiesen werden, allerdings unter Benutzung der Tatsache, daß $\zeta(s)$ auf der Geraden $\sigma = 1$ keine Nullstelle hat (3. Abschnitt).

Im 1. Abschnitt soll hier das Franelsche Kriterium auf die Reihen $\Sigma \sigma(n; h; w) x^n$, falls alle w_r reell sind und ein größtes w existiert, angewandt und dabei die Grenzen des Kriteriums noch einmal deutlich gemacht werden. Im letzten, 7. Abschnitt wird ein Satz über Dirichletsche Reihen bewiesen, der parallel zum Franelschen Potenzreihensatz ist und nicht bloß das Franelsche Kriterium liefert, sondern z. B. auch den Fall $\Sigma d(n) x^n$ und $\Sigma \sigma_u(n) x^n$ für rein imaginäres u umfaßt.

Der Übergang nun von den hier auftretenden Dirichletschen Reihen $f_0(s)$ usf. zu den Potenzreihen kann in den meisten Fällen mit Hilfe des Fatou-Rieszschen und eines Knoppschen[4]) Satzes erfolgen, viel einfacher aber durch den elementaren, wohl schon in irgendeiner Form bekannten Satz I des 2. Abschnittes, der eine Beziehung herstellt zwischen dem Regularitätsbereich der Funktion $f(s)$, welche in einer Halbebene durch die Dirichletsche Reihe $\Sigma a_n n^{-s}$ darstellbar sein möge, und dem Verhalten der Potenzreihe $\Sigma a_n x^n$ (die also sicher für $|x| < 1$ konvergiert) im Punkte $x = 1$. Wenn nun durch ein hieraus entwickeltes Kriterium (Satz III) aus den analytischen Eigenschaften von $f_0(s)$ usf. die Nichtfortsetzbarkeit der Reihen

$$\sum_{n=1}^{\infty} d_h(n) x^n, \quad \sum_{0<n\equiv\alpha(\mathrm{mod}.k)} d_h(n) x^n, \quad \sum_{0<n\equiv\alpha(\mathrm{mod}.k)} d_h(n) x^n + \sum_{0<n\equiv-\alpha(\mathrm{mod}.k)} d_h(n) x^n$$

für $h \geqq 2$ über den Einheitskreis sich ergibt, so folgt zunächst noch nicht dasselbe für die Reihen $\Sigma d_h(n) x^n \cos 2\pi vn$, $\Sigma d_h(n) x^n \sin 2\pi vn$. Das muß vielmehr besonders gezeigt werden und geschieht im Falle $h = 2$ für irrationales v unter Verwendung eines Chowla-Walfiszschen Ergebnisses und für rationales v, im Falle $h > 2$ nur für rationales v. Denn aus der Nichtfortsetzbarkeit der Reihe $\Sigma a_n x^n$ über den Einheitskreis folgt zwar natürlich auch die der Reihe $\Sigma a_n x^n e^{2\pi inv}$, keineswegs aber die der Reihen $\Sigma a_n x^n \cos 2\pi nv$, $\Sigma a_n x^n \sin 2\pi nv$, wie ein, vielleicht noch nicht bekanntes, Gegenbeispiel zeigt; dessen Kern habe ich von Herrn Heilbronn, dem ich hierfür und für manche andere bei der Anfertigung dieser Arbeit erfolgte Hilfe meinen besten Dank ausspreche.

1. Die Anwendung des Franelschen Kriteriums.

Es sei r ganz, $1 \leqq r < h$, es bedeute $\sigma(n; w_1)$ den Wert n^{w_1}, also $d_1(n) = \sigma(n; 0) = 1$, dann folgt aus der Definition

$$(1, 1) \quad \sigma(n; w_1, w_2, \ldots, w_h) = \sum_{\nu\tau=n} \sigma(\nu; w_1, w_2, \ldots, w_r)\, \sigma(\tau; w_{r+1}, w_{r+2}, \ldots, w_h)\,,$$

wobei ν alle Teiler von n durchläuft; ferner ist

[4]) Knopp, a. a. O.[3]), Satz 12, S. 313.

$$\frac{\sigma(n; w_1, w_2, \ldots, w_h)}{n^{w_1}} = \sum_{\delta_1\delta_2\cdots\delta_h=n} \frac{\delta_1^{w_1}\delta_2^{w_2}\cdots\delta_h^{w_h}}{\delta_1^{w_1}\delta_2^{w_1}\cdots\delta_h^{w_1}} = \sigma(n; 0, w_2 - w_1, \ldots, w_h - w_1).$$

Es existiere nun unter den Größen $\Re(w_i)$ eine größte, etwa $\Re(w_1)$. Nimmt man in (1, 1) $r = 1$, so folgt, da $\sigma(\nu; w_1) = \nu^{w_1} = n^{w_1}\tau^{-w_1}$ ist,

$$(1, 2) \qquad \sigma(n; h; w)\, n^{-w_1} = \sum_{\tau|n} \sigma(\tau; w_2 - w_1, w_3 - w_1, \ldots, w_h - w_1).$$

In dem Franelschen Satze kann man also wählen:

$$a_m = \sigma(m; h; w)\, m^{-w_1}, \qquad b_n = \sigma(n; w_2 - w_1, \ldots, w_h - w_1).$$

Es ist

$$\sum_{n=1}^{\infty} \frac{b_n}{n^s} = \sum_{\delta_2, \delta_3, \ldots, \delta_h=1}^{\infty} \frac{\delta_2^{w_2-w_1}}{\delta_2^s} \cdot \frac{\delta_3^{w_3-w_1}}{\delta_3^s} \cdots \frac{\delta_h^{w_h-w_1}}{\delta_h^s} = \prod_{\nu=2}^{h} \zeta(s + w_1 - w_\nu).$$

Jeder Faktor der rechten Seite ist, da $\Re(w_1 - w_\nu) > 0$, eine für $s = 1$ absolut konvergente Dirichletsche Reihe; daher ist auch $\sum_n \frac{b_n}{n}$ und jede Teilreihe davon absolut konvergent, also auch jede Reihe $\sum_n \frac{b_{kn+l}}{kn+l}$. Es seien nun noch alle w reell, dann ist jedes $b_n > 0$, also auch $\sum_n \frac{b_{kn}}{kn} > 0$; folglich ist jede primitive k-te Einheitswurzel eine singuläre Stelle der Funktion

$$F(x) = \sum_{n=1}^{\infty} \sigma(n; h; w) n^{-w_1} x^n, \quad \text{also auch von} \quad \Phi(x) = \sum_{n=1}^{\infty} \sigma(n; h; w)\, x^n$$

nach einem Knoppschen Satze[4]). Die Konvergenz der beiden Reihen *im* Einheitskreise folgte allgemein aus den Voraussetzungen des Franelschen Satzes. Da nun die primitiven Einheitswurzeln auf dem Einheitskreise dicht liegen, ist dieser die natürliche Grenze der Funktion $\Phi(x)$. — Der Beweis ist hier ähnlich geführt wie von Knopp im Falle $h = 2$. Das Kriterium versagt also sicher, wenn kein größtes $\Re(w_i)$ existiert, also z. B. im wichtigsten Falle $w_1 = w_2 = \cdots = w_h = 0$, $\sigma(n; h; 0) = d_h(n)$.

2. Dirichletsche Reihen und Potenzreihen.

Die Reihe $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ möge eine endliche Konvergenzabszisse besitzen; sie sei für $\sigma > \sigma_0 \geqq 0$, $s = \sigma + it$, absolut konvergent, und es sei $g(x) = \sum_{n=1}^{\infty} a_n x^n$. Dann ist bekanntlich für $\sigma > \sigma_0 \geqq 0$

$$(2, 1) \quad f(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} g(e^{-u}) u^{s-1}\, du, \quad \text{auf Grund von} \quad n^{-s} = \frac{1}{\Gamma(s)} \int_0^{\infty} e^{-nu} u^{s-1}\, du.$$

Es sei nun die h-te Abteilung von $g(x)$ für $0 < x < 1$ beschränkt.

a) $h = 0$. Dann ist $|g(x)| < A$ für $0 \leqq x < 1$, also auch $|g(x)| \leqq xA'$, $|g(e^{-u})| \leqq A'e^{-u}$ für $u > 0$. Es sei $N > 1$, dann ist, da $g(e^{-u})$ für $N^{-1} < u < N$ sicher stetig ist,

$$\int_{N^{-1}}^{N} g(e^{-u})\, u^{s-1}\, du$$

eine ganze Funktion von s. Nun ist für $0 < \varepsilon \leqq \sigma \leqq \varepsilon^{-1}$

$$\left| \int_N^{\infty} g(e^{-u})\, u^{s-1}\, du \right| \leqq A' \int_N^{\infty} e^{-u} u^{\frac{1}{\varepsilon}-1}\, du, \qquad \left| \int_0^{N^{-1}} \right| < A \int_0^{N^{-1}} u^{\varepsilon-1}\, du;$$

beide Integrale konvergieren bei festem ε gleichmäßig in s für $N \to \infty$ gegen 0, daher ist $f(s)$ für $\sigma > 0$ regulär.

b) $h > 0$. Man setze $f_1(s) = \Sigma a_n n^{h-s} = f(s-h)$, $g_1(x) = \Sigma a_n n^h x^n$. Falls $|g_1(x)|$ für $0 < x < 1$ beschränkt ist, so ist sicher auf Grund des eben Bewiesenen $f_1(s)$ für $\sigma > 0$, also $f(s') = f(s-h)$, wenn $s' = \sigma' + it'$, $s' = s - h$ gesetzt wird, für $\sigma' > -h$ regulär. Nun gibt es aber rationale Zahlen $\alpha_{h,1}, \alpha_{h,2}, \ldots, \alpha_{h,h}$ so, daß

$$n^h = \sum_{r=1}^{h} \alpha_{h,r} \binom{n}{r}, \quad \text{also} \quad g_1(x) = \sum_{r=1}^{h} \alpha_{h,r} \sum_{n=1}^{\infty} a_n \binom{n}{r} x^n = \sum_{r=1}^{h} \alpha_{h,r} \frac{x^r}{r!} g^{(r)}(x)$$

ist. Da aber $|g^{(h)}(x)|$ für $0 < x < 1$ beschränkt ist, so auch $|g^{(h-1)}(x)|$, weil

$$g^{(h-1)}(x) = (h-1)!\, a_{h-1} + \int_0^x g^{(h)}(t)\, dt,$$

entsprechend $|g^{(h-2)}(x)|$ usf., also auch $|g_1(x)|$. So folgt

Satz I. *Wenn die Dirichletsche Reihe $\sum_{n=1}^{\infty} a_n n^{-s}$ eine endliche Konvergenzabszisse besitzt und im Konvergenzgebiet gleich $f(s)$ ist, und wenn die h-te Ableitung der Potenzreihe $\Sigma a_n x^n$ für $0 < x < 1$ beschränkt ist, ist $f(s)$ für $\sigma > -h$ regulär.*

Wie sich durch ein- bzw. mehrfache partielle Integration zeigen läßt, ist übrigens der Satz auch für negative ganze Werte von h richtig, wenn man unter $g^{(h)}(x)$ dann das $|h|$-fache Integral von $g(x)$ versteht.

Folgerungen aus diesem Satze:

Satz II. *Die Reihe $\sum_{n=1}^{\infty} a_n n^{-s}$ besitze eine endliche Konvergenzabszisse und sei in der Konvergenzhalbebene gleich $f(s)$. Wenn die Potenzreihe $g(x) = \sum_{n=1}^{\infty} a_n x^n$ im Punkte $x = 1$ regulär ist, ist $f(s)$ eine ganze Funktion.*

Denn jede Ableitung der Potenzreihe ist dann für $0 < x < 1$ beschränkt. Wenn daher die Reihe $\Sigma a_n n^{-s}$ eine endliche Konvergenzabszisse besitzt und die Funktion $f(s)$ im Endlichen mindestens eine Singularität hat, kann die Potenzreihe $g(x)$ im Punkte $x = 1$ nicht regulär sein. Und schließlich:

Satz III. *Es gehöre v zu einer Menge von Zahlen des Intervalles $(0, 1)$, die in diesem Intervalle überall dicht sei, $\sum_{n=1}^{\infty} a_n n^{-s}$ besitze eine endliche Konvergenzabszisse und jede Funktion $f(s, v) = \sum_{n=1}^{\infty} a_n n^{-s} e^{2\pi i n v}$ mindestens eine Singularität im Endlichen. Dann hat die Potenzreihe $g(x) = \Sigma a_n x^n$ den Einheitskreis (in dessen Innerem sie regulär ist) zur natürlichen Grenze.*

Der Satz II ist natürlich nicht umkehrbar, wie das Beispiel[5]) der Funktionen $f(s) = \Sigma d(n) n^{-s} \sin 2\pi a n$, $g(x) = \Sigma d(n) x^n \sin 2\pi a n$ zeigt; wenn nämlich a beliebig rational, aber nicht die Hälfte einer ganzen Zahl ist, ist $f(s)$ ganz, $g(x)$ aber im Punkte $x = 1$ und sogar in jedem Punkte des Einheitskreises singulär, wie noch gezeigt werden wird. Aber folgende Umkehrung des Satzes I gilt: *Die Reihe $\sum_{n=1}^{\infty} a_n n^{-s}$ möge ein Konvergenzgebiet besitzen und sei dort gleich $f(s)$, $f(s)$ sei für $\sigma > -b$ regulär und in dieser Halbebene von der Form $\boldsymbol{O}(e^{\varepsilon|t|})$ für jedes $\varepsilon > 0$, $|t| \to \infty$; b sei > 0, h die größte ganze Zahl $< b$, $r = 0, 1, 2, \ldots, h$. Dann existiert für jedes r, falls $g(x) = \Sigma a_n x^n$ und $0 < \varphi < \frac{\pi}{2}$, φ sonst beliebig festgelegt ist, $\lim_{x \to 1} g^{(r)}(x)$ gleichmäßig im Winkelraum $|\arg(1-x)| \leqq \varphi$.*

[5]) Vgl. Abschnitt 4, Gleichung (4, 4′), und Abschnitt 6, C.

Natürlich ist also auch $|g^{(r)}(x)|$ für $0 < x < 1$ beschränkt.

Der Beweis dieses elementaren, wohl schon in irgendeiner Form bekannten Satzes folgt unmittelbar aus der Formel

$$(2,2) \qquad g(x) = \frac{1}{2\pi i} \int_{\sigma_0 - i\infty}^{\sigma_0 + i\infty} \left(\log \frac{1}{x}\right)^{-s} \Gamma(s)\, f(s)\, ds\,,$$

die für $0 < |x| < 1$, $\sigma_0 >$ Abszisse der absoluten Konvergenz und > 0 gilt, wobei $\left|\arg \log \frac{1}{x}\right| < \frac{\pi}{2}$ gewählt ist. Zunächst sei $h = 0$, also $-1 \leqq -b < 0$. Dann ist

$$(2,3) \qquad \Gamma(s) = \boldsymbol{O}\left(|t|^{\sigma - \frac{1}{2}} e^{-\frac{\pi}{2}|t|}\right),\ f(s) = \boldsymbol{O}(e^{\varepsilon|t|})$$

gleichmäßig für $-b < \sigma \leqq \sigma_0$. Nun sei $0 > \sigma_1 > -b$, dann kann man also den Integrationsweg in die Gerade $s = \sigma_1 + it$ verlegen:

$$g(x) = f(0) + F(x);\quad F(x) = \frac{1}{2\pi i} \int_{\sigma_1 - i\infty}^{\sigma_1 + i\infty} \left(\log \frac{1}{x}\right)^{-s} \Gamma(s)\, f(s)\, ds\,.$$

Man denke sich jetzt durch den Punkt $x = 1$ die beiden Strahlen gezogen, die mit der positiven reellen Achse die Winkel $\pi \pm \varphi$ bilden, und vom Punkte 0 auf jeden das Lot gefällt. Es bedeute jetzt x nur noch irgendeinen Punkt im Inneren oder auf dem Rande des so entstandenen Vierecks, ausgenommen die Punkte 0 und 1. Dann ist

$$(2,4) \qquad |\arg x| \leqq \frac{\pi}{2} - \varphi,\quad |x| < 1,\quad |\arg (1-x)| \leqq \varphi < \frac{\pi}{2},$$

$$|x| \leqq \frac{\sin \varphi}{\sin (\varphi + |\arg x|)}\,.$$

Es sei nun $\log \frac{1}{x} = ye^{-i\psi}$, $y > 0$, $|\psi| < \frac{\pi}{2}$, dann ist

$$y = \sqrt{\log^2 |x| + \arg^2 x},$$

$$|\operatorname{tg} \psi| = \left|\frac{\arg x}{-\log |x|}\right| < \frac{|\arg x|}{1 - |x|} \leqq \frac{|\arg x| \sin (\varphi + |\arg x|)}{2 \sin \frac{|\arg x|}{2} \cos\left(\varphi + \frac{|\arg x|}{2}\right)} < \frac{2}{\cos\left(\frac{\pi}{4} + \frac{\varphi}{2}\right)}$$

mit Rücksicht auf (2, 4), daher liegt $\frac{\pi}{2} - |\psi|$ über einer festen positiven Zahl. Zufolge der letzten und ersten Ungleichung von (2, 4) strebt mit $x \to 1$ gleichmäßig $\arg x$ gegen 0, daher auch y, und weil

$$|F(x)| < \frac{1}{2\pi} y^{-\sigma_1} \int_{-\infty}^{\infty} e^{|t\psi|}\, |\Gamma(\sigma_1 + it)\, f(\sigma_1 + it)|\, dt\,,$$

so strebt mit Rücksicht auf (2, 3) auch $F(x)$ gleichmäßig gegen 0 und daher $g(x)$ gegen $f(0)$, q. e. d.

Im Falle $h > 0$ betrachte man die Funktionen $f_r(s) = f(s - r)$, $g_r(x) = \Sigma a_n n^r x^n$ und verfahre ähnlich wie beim Beweise des Satzes I. Falls ε (vgl. 2, 3) nach unten beschränkt ist, $\varepsilon \geqq \varepsilon_0 > 0$, so ergibt sich für φ eine Beschränkung nach oben, $0 < \varphi < \varphi_0 = \frac{\pi}{2} - \varepsilon_0$.

3. Die Reihe $\sum_{n=1}^{\infty}\sigma_u(n)x^n$.

Mit Hilfe des Satzes III läßt sich nun dieser bereits bekannte Fall rasch auf dem neuen Wege behandeln. Setzt man

$$(3,1)\qquad \zeta_1(z;\alpha)=\frac{1}{2}\sum_{\substack{n=-\infty\\ n+\alpha\neq 0}}^{\infty}\frac{1}{|n+\alpha|^z},\qquad \zeta_2(z;\alpha)=\sum_{n=1}^{\infty}n^{-z}\cos 2\pi\alpha n,$$

$$(3,2)\qquad \eta_1(z;\alpha)=\frac{1}{2}\sum_{\substack{n=-\infty\\ n+\alpha\neq 0}}^{\infty}\frac{n+\alpha}{|n+\alpha|^{z+1}},\qquad \eta_2(z;\alpha)=\sum_{n=1}^{\infty}n^{-z}\sin 2\pi\alpha n,$$

— aus Satz II folgt übrigens sofort die wohlbekannte Tatsache, daß $\zeta_2(z;\alpha)$ für $0<\alpha<1$ und $\eta_2(z;\alpha)$ immer eine ganze Funktion von z ist —, so ist [6])

$$\begin{aligned}\mathsf{Z}_1(s;v;w)&=\sum_{n=1}^{\infty}n^{-s-w}\sigma_{2w}(n)\cos 2\pi vn=c^{-s-w}\sum_{m=1}^{c}\zeta_1\left(s+w;\ \frac{m}{c}\right)\zeta_2\left(s-w;\ \frac{m'}{c}\right)\\&=F(s;v;w)+c^{1-2s}\zeta(s+w)\zeta(s-w),\\F(s;v;w)&=c^{-s-w}\sum_{m=1}^{c-1}\left(\zeta_1\left(s+w;\ \frac{m}{c}\right)-\zeta(s+w)\right)\zeta_2\left(s-w;\ \frac{m'}{c}\right),\end{aligned}$$

wobei $v=\frac{a}{c}$ beliebig rational, w beliebig komplex, $m'\equiv am\ (\mathrm{mod.}\ c)$ und F eine ganze Funktion von s und w ist; auch $\mathsf{Z}_2(s;v;w)=\sum_{n=1}^{\infty}n^{-s-w}\sigma_{2w}(n)\sin 2\pi vn$ ist eine ganze Funktion von s und w, daher auch

$$\sum_{n=1}^{\infty}n^{-s-w}\sigma_{2w}(n)\,e^{2i\pi vn}-c^{1-2s}\zeta(s+w)\zeta(s-w).$$

Nun ist aber, da $\zeta(z)$ an der Stelle $z=1$ einen Pol erster Ordnung hat, das Produkt $\zeta(s+w)\zeta(s-w)$ mindestens an einer der beiden Stellen $s=1+w$ oder $s=1-w$ singulär, da sonst $\zeta(1+2w)$ und $\zeta(1-2w)$ gleichzeitig verschwinden, also die Summe zweier Nullstellen der ζ-Funktion gleich 2 sein müßte, während doch bekanntlich der reelle Teil jeder Nullstelle <1 ist. Folglich hat die Funktion $f(s')=\sum_{n=1}^{\infty}n^{-s'}\sigma_{2w}(n)\,e^{2\pi ivn}$ für jedes rationale v im Endlichen mindestens eine Singularität, daher hat nach Satz III die Reihe $\Sigma\sigma_u(n)x^n$ den Einheitskreis zur natürlichen Grenze, und zwar für beliebiges komplexes u.

4. Die Verwandten der Potenzen von $\zeta(s)$.

Es sei $\mathfrak{a}=0$ oder 1. Dann ist bekanntlich (s. auch Verf., a. a. O. [2])) $\zeta(z;\alpha)=\sum_{n=0}^{\infty}(n+\alpha)^{-z}$ für $0<\alpha\leqq 1$, gleich $\zeta(z)$ für $\alpha=0$, $\zeta(z;\alpha)-\frac{1}{z-1}$ eine ganze Funktion von z, $2\zeta_1(z;\alpha)=\zeta(z;\alpha)+\zeta(z;1-\alpha)$,

$$\zeta_1(z;\alpha)=\frac{1}{z-1}+H(z,\alpha),\ H(z,\alpha)\text{ eine ganze Funktion von }z,$$

$$\zeta_2(z;\alpha)=\zeta(z)\text{ für }\alpha\equiv 0\ (\mathrm{mod.}\ 1),\text{ ganz für }\alpha\not\equiv 0\ (\mathrm{mod.}\ 1),$$

η_1 und η_2 je eine ganze Funktion von z,

$$(4,01)\qquad \zeta_1(z;\alpha)\pi^{-\frac{z}{2}}\Gamma\left(\frac{z}{2}\right)=\pi^{\frac{z-1}{2}}\Gamma\left(\frac{1-z}{2}\right)\zeta_2(1-z;\alpha),$$

$$(4,02)\qquad \eta_1(z;\alpha)\pi^{-\frac{z}{2}}\Gamma\left(\frac{z+1}{2}\right)=\pi^{\frac{z-1}{2}}\Gamma\left(\frac{2-z}{2}\right)\eta_2(1-z;\alpha).$$

Es sei $\alpha = \frac{\beta}{k}$ rational, $k > 0$, ferner

$$f_0(z) = 2k^{-z}\,\zeta_1\left(z;\,\frac{\beta}{k}\right) = \sum_{\substack{n\equiv\beta\,(\mathrm{mod.}\,k)\\ n>0}} n^{-z} + \sum_{\substack{n\equiv-\beta\,(\mathrm{mod.}\,k)\\ n>0}} n^{-z},$$

$$f_1(z) = 2k^{-z}\,\eta_1\left(z;\,\frac{\beta}{k}\right) = \sum_{\substack{n\equiv\beta\,(\mathrm{mod.}\,k)\\ n>0}} n^{-z} - \sum_{\substack{n\equiv-\beta\,(\mathrm{mod.}\,k)\\ n>0}} n^{-z},$$

$$\varphi_0(z) = \frac{2}{\sqrt{k}}\,\zeta_2\left(z;\,\frac{\beta}{k}\right), \qquad \varphi_1(z) = \frac{2}{\sqrt{k}}\,\eta_2\left(z;\,\frac{\beta}{k}\right).$$

Dann sind φ_0 und φ_1 für $\Re(z) > 1$ durch absolut konvergente Dirichletsche Reihen darstellbar, f_0 und f_1 sind Funktionen der in den Gleichungen (4a) und (4b) aufgestellten Form (s. Einleitung) mit z und β anstelle von s und α im Falle $h = 1$, da $d_1(n) = 1$ ist, und aus den Gleichungen (4, 01) und (4, 02) folgt die Gültigkeit der Funktionalgleichung (4c) im Falle $h = 1$. — Setzt man $z = s - w_1$, $\sigma(n; w_1) = n^{w_1}$, wieder $\mathfrak{a} = 0$ oder 1, $f_\mathfrak{a}(z) = f_\mathfrak{a}(s - w_1) = {}_1f_\mathfrak{a}(s; w_1)$, also gleich $\Sigma\sigma(|n|; w_1)\,|n|^{-s}$ bzw. $\Sigma\sigma(|n|; w_1)\,n\,|n|^{-s-1}$, wobei über alle von 0 verschiedenen Zahlen summiert wird, die $\equiv \beta\,(\mathrm{mod.}\,k)$ sind, setzt man ferner $\varphi_\mathfrak{a}(z + w_1) = {}_1\varphi_\mathfrak{a}(z; w_1)$, so ist ${}_1f_1$ und ebenso $(s - w_1 - 1)\;{}_1f_0(s; w_1)$ eine ganze Funktion von s und w_1, ${}_1\varphi_\mathfrak{a}$ ist für $\Re(z) > 1 - \Re(w_1)$ durch eine absolut konvergente Dirichletsche Reihe darstellbar, und es gilt die allgemeinere Gleichung:

$${}_1f_\mathfrak{a}(s; w_1)\,\Gamma\left(\frac{s + \mathfrak{a} - w_1}{2}\right)\left(\frac{\pi}{k}\right)^{-\frac{s-w_1}{2}} = {}_1\varphi_\mathfrak{a}(1 - s; w_1)\,\Gamma\left(\frac{1 + \mathfrak{a} - s + w_1}{2}\right)\left(\frac{\pi}{k}\right)^{\frac{s-w_1-1}{2}}.$$

Setzt man

$$f_0(s; w_1, \ldots, w_h) = \sum_{\substack{n\equiv\alpha\,(\mathrm{mod.}\,k)\\ n\neq 0}} \frac{\sigma(|n|; h; w)}{|n|^s}, \quad f_1(s; w_1, \ldots, w_h) = \sum_{\substack{n\equiv\alpha\,(\mathrm{mod.}\,k)\\ n\neq 0}} \frac{\sigma(|n|; h; w)\,n}{|n|^{s+1}},$$

wobei die Reihen für $\sigma > 1 + \mathrm{Max}\,(\Re(w_1), \ldots, \Re(w_h))$ absolut konvergieren, so sind

$$f_0(s; w_1, \ldots, w_h)\prod_{r=1}^{h}(s - w_r - 1) \quad \text{und} \quad f_1(s; w_1, \ldots, w_h)$$

ganze Funktionen aller vorkommenden Variablen, und es ist

$$(4,1)\qquad f_\mathfrak{a}(s; w_1, \ldots, w_h)\left(\frac{\pi}{k}\right)^{\frac{1}{2}\sum_{r=1}^{h} w_r - \frac{hs}{2}} \prod_{r=1}^{h}\Gamma\left(\frac{s + \mathfrak{a} - w_r}{2}\right)$$

$$= \varphi_\mathfrak{a}(1 - s; w_1, w_2, \ldots, w_h)\left(\frac{\pi}{k}\right)^{\frac{h}{2}(s-1) - \frac{1}{2}\sum_{r=1}^{h} w_r} \prod_{r=1}^{h}\Gamma\left(\frac{1 - s + \mathfrak{a} + w_r}{2}\right),$$

wobei die Funktion $\varphi_\mathfrak{a}(s; w_1, w_2, \ldots, w_h)$ für $\Re(s) > 1 - \mathrm{Min}\,(\Re(w_1), \ldots, \Re(w_h))$ durch eine absolut konvergente Dirichletsche Reihe darstellbar ist. — Für das Weitere werde ich mich auf den wichtigsten Fall $w_1 = w_2 = \cdots = w_h = 0$ und somit auf den Beweis der Funktionalgleichung (4c) und der anderen, bereits in der Einleitung formulierten, Behauptungen beschränken. Der allgemeine Fall ist nicht viel schwieriger. Der Beweis könnte mit Hilfe der Charaktere, ebenso etwa wie bei den Kluyverschen Reihen[7]), geführt werden. Erheblich einfacher aber ist ein direkter Weg. Der Satz ist für $h = 1$ richtig, er möge für irgendein ganzzahliges $h \geqq 1$ gelten, sodaß die Funktionen

---

[6]) H. Kober, a. a. O. [2]), II. Teil, S. 73, im Falle $w = 0$; der allgemeine Fall ergibt sich leicht.

[7]) Landau, Handbuch der Lehre von der Verteilung der Primzahlen, § 192 u. f., oder ähnlich wie in § 103.

$$f_0(s;h;k,\alpha)=\sum_{\substack{n\equiv\alpha\,(\mathrm{mod}.\,k)\\ n\neq 0}} d_h(|n|)\,|n|^{-s},\qquad f_1(s;h;k,\alpha)=\sum_{\substack{n\equiv\alpha\,(\mathrm{mod}.\,k)\\ n\neq 0}} n\,d_h(|n|)\,|n|^{-s-1}$$

der Funktionalgleichung (4c) genügen, die dort auftretende Funktion $\varphi_a(s)$ möge für $\sigma>1$ durch eine absolut konvergente Dirichletsche Reihe darstellbar sein, und $(s-1)^h f_0$ und f_1 mögen ganze Funktionen sein. Es sei nun

$$f_0(s;h+1;k,\alpha)=\sum_{\substack{n\equiv\alpha\,(\mathrm{mod}.\,k)\\ n\neq 0}} d_{h+1}(|n|)\,|n|^{-s}=\sum_{\substack{n\equiv\alpha\,(\mathrm{mod}.\,k)\\ n>0}} d_{h+1}(n)\,n^{-s}+\sum_{\substack{n\equiv-\alpha\,(\mathrm{mod}.\,k)\\ n>0}} d_{h+1}(n)\,n^{-s}.$$

Es ist nach (1, 1) $\quad d_{h+1}(n)=\sum_{\substack{\nu\tau=n\\ \nu>0,\ \tau>0}} d_h(\nu)$, also $\sum_{\substack{n\equiv\alpha\,(\mathrm{mod}.\,k)\\ n>0}} d_{h+1}(n)\,n^{-s}=\sum_{\substack{\nu\tau\equiv\alpha\,(\mathrm{mod}.\,k)\\ \nu>0,\ \tau>0}} d_h(\nu)\,\nu^{-s}\tau^{-s}$.

Man erhält genau alle zulässigen Werte von ν und τ, indem man ν in jeder der k arithmetischen Reihen $\nu\equiv m\,(\mathrm{mod}.\,k)$, $m=1,2,\ldots,k$, alle positiven Zahlen durchlaufen läßt und bei festem m die Größe τ alle positiven Zahlen jeder der $j(m)$ Reihen $\tau\equiv m'_r\,(\mathrm{mod}.\,k)$. Hierbei durchläuft $m'_r=m'_r(m)$ alle mod. k verschiedenen Lösungen x der Kongruenz $mx\equiv\alpha\,(\mathrm{mod}.\,k)$, deren Lösungszahl $=j(m)$ sein soll; ist $j(m)=0$, so fällt die entsprechende Reihe $\nu\equiv m\,(\mathrm{mod}.\,k)$ aus. So ist

$$\sum_{\substack{n\equiv\alpha\,(\mathrm{mod}.\,k)\\ n>0}} d_{h+1}(n)\,n^{-s}=\sum_{m=1}^{k}\sum_{\substack{\nu\equiv m\\ \nu>0}}\frac{d_h(\nu)}{\nu^s}\sum_{r=1}^{j(m)}\sum_{\substack{\tau\equiv m'_r(m)\\ \tau>0}}\tau^{-s}=\sum_{m=1}^{k}\sum_{\substack{\nu\equiv -m\\ \nu>0}}\frac{d_h(\nu)}{\nu^s}\sum_{r=1}^{j(m)}\sum_{\substack{\tau\equiv -m'_r(m)\\ \tau>0}}\tau^{-s};$$

$$\sum_{\substack{n\equiv-\alpha\,(\mathrm{mod}.\,k)\\ n>0}} d_{h+1}(n)\,n^{-s}=\sum_{m=1}^{k}\sum_{\substack{\nu\equiv m\\ \nu>0}}\frac{d_h(\nu)}{\nu^s}\sum_{r=1}^{j(m)}\sum_{\substack{\tau\equiv -m'_r(m)\\ \tau>0}}\tau^{-s}=\sum_{m=1}^{k}\sum_{\substack{\nu\equiv -m\\ \nu>0}}\frac{d_h(\nu)}{\nu^s}\sum_{r=1}^{j(m)}\sum_{\substack{\tau\equiv m'_r(m)\\ \tau>0}}\tau^{-s},$$

wobei für $j(m)=0$ die innersten Summen den Wert 0 haben. Nun folgt

$$(4,2)\quad f_0(s;h+1;k,\alpha)=\sum_{m=1}^{k}\sum_{\substack{\nu\equiv m\\ \nu>0}}\frac{d_h(\nu)}{\nu^s}\sum_{r=1}^{j(m)}\sum_{\substack{\tau\equiv m'_r(m)\\ \tau\gtrless 0}}|\tau|^{-s}=\sum_{m=1}^{k}\sum_{\substack{\nu\equiv -m\\ \nu>0}}\frac{d_h(\nu)}{\nu^s}\sum_{r=1}^{j(m)}\sum_{\substack{\tau\equiv m'_r(m)\\ \tau\gtrless 0}}|\tau|^{-s}$$

$$=\frac{1}{2}\sum_{m=1}^{k}\sum_{\substack{\nu\equiv m\\ \nu\gtrless 0}} d_h(|\nu|)\,|\nu|^{-s}\sum_{r=1}^{j(m)}\sum_{\substack{\tau\equiv m'_r(m)\\ \tau\gtrless 0}}|\tau|^{-s}=\frac{1}{2}\sum_{m=1}^{k} f_0(s;h;k,m)\sum_{r=1}^{j(m)} f_0(s;1;k,m'_r(m)).$$

Die rechte Seite ist eine endliche Summe von Produkten. Nun ist sowohl $(s-1)^h f_0(s;h;k,m)$ wie $(s-1)\,f_0(s;1;k,m')$ eine ganze Funktion, also auch $(s-1)^{h+1} f_0(s;h+1;k,\alpha)$. Da aber $f_0(s;h;k,m)$ der Funktionalgleichung (4c) genügt, ebenso $f_0(s;1;k,m')$ mit $h=1$, und da durch Multiplikation zweier solcher Funktionalgleichungen vom Grade h bzw. 1 eine solche vom Grade $h+1$, durch Addition zweier solcher von gleichem Grade wieder eine von demselben Grade entsteht, genügt $f_0(s;h+1;k,\alpha)$ einer Funktionalgleichung (4c) vom Grade $h+1$ mit $\mathfrak{a}=0$. Die Funktion φ_0 ist von der verlangten Art, da sowohl die Summe wie das Produkt zweier für $\sigma>1$ absolut konvergenter Dirichletscher Reihen wieder für $\sigma>1$ absolut konvergiert.

Entsprechend erhält man für die Funktion

$$(4,3)\quad f_1(s;h+1;k,\alpha)=\sum_{\substack{n\equiv\alpha\,(\mathrm{mod}.\,k)\\ n>0}} d_{h+1}(n)\,n^{-s}-\sum_{\substack{n\equiv-\alpha\\ n>0}}=\sum_{m=1}^{k}\sum_{\substack{\nu\equiv m\\ \nu>0}}\frac{d_h(\nu)}{\nu^s}\sum_{r=1}^{j(m)}\sum_{\substack{\tau\equiv m'_r(m)\\ \tau\neq 0}}\tau\,|\tau|^{-s-1}$$

$$=-\sum_{m=1}^{k}\sum_{\substack{\nu\equiv -m\\ \nu>0}}=\frac{1}{2}\sum_{m=1}^{k}\sum_{\substack{\nu\equiv m\\ \nu\neq 0}} d_h(|\nu|)\nu\,|\nu|^{-s-1}\sum_{r=1}^{j(m)}\sum_{\substack{\tau\equiv m'_r(m)\\ \tau\neq 0}}\tau\,|\tau|^{-s-1}$$

$$=\frac{1}{2}\sum_{m=1}^{k} f_1(s;h;k,m)\sum_{r=1}^{j(m)} f_1(s;1;k,m'_r(m))$$

und entsprechend die verlangten Eigenschaften; so ist auch der Fall $\mathfrak{a} = 1$ bewiesen. Man erhält für die Funktion $\varphi_{\mathfrak{a}}(s)$ die Reihe $\sum_1^\infty a_{n,\mathfrak{a}} n^{-s}$,

$$a_{n,\binom{0}{1}} = 2k^{-\frac{h}{2}} \sum_{\substack{m_1, m_2, \ldots, m_h \\ m_1 m_2 \cdots m_h \equiv \alpha \,(\mathrm{mod}.\, k)}} \sum_{\substack{r_1, r_2, \ldots, r_h \\ r_1 r_2 \cdots r_h = n}} \prod_{j=1}^{h} \begin{matrix}\cos \\ \sin\end{matrix} (2\pi m_j r_j k^{-1}) .$$

Ferner folgt leicht [8]):

Es sei $f(s) = \sum_1^\infty a_n n^{-s}$, *es existiere eine ganze Zahl* $k > 0$ *so, daß für jedes ganze* $n > 0$, *jedes positive* $m < k$

$$a_{n+k} d_h(n) = a_n d_h(n + k), \qquad a_m d_h(k - m) = a_{k-m} d_h(m)$$

ist. Dann ist $(s-1)^h f(s)$ *eine ganze Funktion, und* $f(s)$ *genügt einer Funktionalgleichung* (4c) *mit* $\mathfrak{a} = 0$. *Wenn aber*

$$a_{n+k} d_h(n) = a_n d_h(n + k), \qquad a_m d_h(k - m) = - a_{k-m} d_h(m), \qquad a_k = 0$$

ist, so ist $f(s)$ *ganz und genügt einer Funktionalgleichung* (4c) *mit* $\mathfrak{a} = 1$.

Es sollen jetzt noch zwei bestimmte Funktionen dieser letzten Art betrachtet werden. Es sei $v = \frac{a}{c}$, $(a, c) = 1$, C das kleinste gemeinschaftliche Vielfache von k und c, $C = kl > 0$. Dann ist

$$(4,4) \qquad \begin{aligned} F_0(s; h; k, \alpha, v) &= \sum_{\substack{n \equiv \alpha \,(\mathrm{mod}.\, k) \\ n \neq 0}} \frac{d_h(|n|)}{|n|^s} \cos 2\pi v n = \sum_{r=0}^{l-1} \sum_{\substack{n \equiv \alpha + rk \,(\mathrm{mod}.\, C) \\ n \neq 0}} d_h(|n|)\, |n|^{-s} \cos 2\pi v n \\ &= \sum_{r=0}^{l-1} \cos (2\pi v(\alpha + rk))\; f_0(s; h; C, \alpha + rk) , \end{aligned}$$

genügt also der Gleichung (4c) mit C an Stelle von k, und $(s-1)^h F_0$ ist ganz, $\mathfrak{a} = 0$. Entsprechend ist

$$(4,4') \qquad \begin{aligned} F_1(s; h; k, \alpha, v) &= \sum_{\substack{n \equiv \alpha \,(\mathrm{mod}.\, k) \\ n \neq 0}} \frac{d_h(|n|)}{|n|^s} \sin 2\pi v |n| = \sum_{r=0}^{l-1} \sum_{\substack{n \equiv \alpha + rk \,(\mathrm{mod}.\, C) \\ n \neq 0}} d_h(|n|)\, n\, |n|^{-s-1} \sin 2\pi v n \\ &= \sum_{r=0}^{l-1} \sin (2\pi v(\alpha + rk))\; f_1(s; h; C, \alpha + rk) , \end{aligned}$$

ist also eine ganze Funktion und genügt der Gleichung (4c) mit $\mathfrak{a} = 1$ und C an Stelle von k. Dieselben Ergebnisse erhält man entsprechend für

$$(4,5) \quad \tilde{F}_0(s; h; k, \alpha, v) = \sum_{\substack{n \equiv \alpha \,(\mathrm{mod}.\, k) \\ n \neq 0}} \frac{d_h(|n|)}{|n|^s} \sin 2\pi v n, \quad \tilde{F}_1(s; h; k, \alpha, v) = \sum_{\substack{n \equiv \alpha \,(\mathrm{mod}.\, k) \\ n \neq 0}} \frac{n d_h(|n|)}{|n|^{s+1}} \cos 2\pi v n,$$

$$(4,6) \quad G_0(s; h; k, \alpha, v) = \sum_{\substack{n \equiv \alpha \,(\mathrm{mod}.\, k) \\ n \neq 0}} \frac{d_h(|n|)}{|n|^s} e^{2i\pi v n}, \qquad G_1(s; h; k, \alpha, v) = \sum_{\substack{n \equiv \alpha \,(\mathrm{mod}.\, k) \\ n \neq 0}} \frac{n d_h(|n|)}{|n|^{s+1}} e^{2i\pi v n} .$$

Besonders einfach ist der Fall $k = 1$, $C = c = l$. Dann ist

$$F_0 = G_0 = 2 \sum_1^\infty \frac{d_h(n)}{n^s} \cos 2\pi v n, \qquad G_1 = i F_1 = 2i \sum_1^\infty \frac{d_h(n)}{n^s} \sin 2\pi v n.$$

Bei der Ableitung der Eigenschaften von f_0 und f_1 schloß man aus den Fällen h und 1 auf den Fall $h + 1$. Genau ebenso kann man auf Grund von (1, 1) aus den Fällen h_1 und h_2

[8]) Dies ist eine Verallgemeinerung eines Hamburgerschen Satzes, vgl. H. Kober, Eine der Riemannschen verwandte Funktionalgleichung, Math. Zeitschr. **39** (1935), S. 630—633, insbesondere Note 1. Der Satz ist aber im Falle $h > 1$ nicht umkehrbar.

auf den Fall $h_1 + h_2$, also aus h und 2 auf $h+2$ schließen. Nun ist

$$\sum_{\substack{n\equiv\alpha\,(\mathrm{mod.}\,k)\\ 0<|n|\leqq x}} d(|n|)\,\mathrm{sign}\,(n) = \sum_{\substack{n\equiv\alpha\,(\mathrm{mod.}\,k)\\ 0<n\leqq x}} d(n) - \sum_{\substack{n\equiv-\alpha\,(\mathrm{mod.}\,k)\\ 0<n\leqq x}} d(n) = \boldsymbol{O}(x^{\frac{1}{3}}\log x)$$

auf Grund eines Ramanujanschen [9]), natürlich stark verbesserungsfähigen, Resultates, also die Reihe $\Sigma n d(|n|)|n|^{-s-1}$, $n \equiv \alpha\,(\mathrm{mod.}\,k)$ und $\neq 0$, für jedes $\sigma > \frac{1}{3}$ konvergent, wenn die Glieder nach der Größe von $|n|$ geordnet sind. Durch dasselbe Verfahren wie in einer früheren Arbeit des Verfassers [10]) erhält man unter Benutzung eines allgemeinen Satzes über das Produkt zweier Dirichletscher Reihen und der Gleichung (4, 3)

$$\sum_{\substack{n\equiv\alpha\,(\mathrm{mod.}\,k)\\ 0<n\leqq x}} d_h(|n|)\,\mathrm{sign}\,(n) = \boldsymbol{O}(x^{\vartheta}), \qquad \sum_{n=1}^{x} d_h(n)\sin 2\pi v n = \boldsymbol{O}(x^{\vartheta})$$

für rationales v, jedes $\vartheta > 1 - \frac{4}{3h}$ im Falle eines geraden h durch Schluß von h auf $h+2$, jedes $\vartheta > 1 - \frac{4}{3h+1}$ im Falle eines ungeraden h durch Schluß von h auf $h+1$. Das sind natürlich nur grobe Ergebnisse. Wendet man aber den Hauptsatz einer Arbeit von Herrn Landau an [11]), dessen Voraussetzungen hier sämtlich erfüllt sind, besonders mit Rücksicht auf (4c), so erhält man schließlich:

$$\sum_{\substack{n\equiv\alpha\,(\mathrm{mod.}\,k)\\ 0<n\leqq x}} d_h(n) - \sum_{\substack{n\equiv-\alpha\,(\mathrm{mod.}\,k)\\ 0<n\leqq x}} d_h(n) = \boldsymbol{O}\left(x^{\frac{h-1}{h+1}}\log^{h-1} x\right), \qquad \sum_{n=1}^{x} d_h(n)\sin 2\pi v n = \boldsymbol{O}\left(x^{\frac{h-1}{h+1}}\log^{h-1} x\right)$$

für $h \geqq 2$ und rationales v. Von genau derselben Größenordnung sind die Fehlerglieder bei den Summen (v beliebig rational)

$$\sum_{\substack{n\equiv\alpha\,(\mathrm{mod.}\,k)\\ 0<n\leqq x}} d_h(n)\cos 2\pi v n, \qquad \sum_{\substack{n\equiv\alpha\,(\mathrm{mod.}\,k)\\ 0<n\leqq x}} d_h(n)\sin 2\pi v n.$$

Zur Bestimmung des Hauptgliedes braucht man auch die Resultate des nächsten Abschnittes.

5. Die Hauptkoeffizienten.

Im Falle $h = 1$ ist

$$\frac{1}{2} f_0(z; 1; k, \beta) = k^{-z}\,\zeta_1\left(z; \frac{\beta}{k}\right) = k^{-z}((z-1)^{-1} + \cdots) = k^{-1}(z-1)^{-1} + \cdots,$$

also der Koeffizient für $2^{-1}f_0(z)$ gleich k^{-1} (s. Anfang von Abschnitt 4).

Im Falle $h = 2$ ist auf Grund von Gleichung (4, 2) und des eben Festgestellten in der Umgebung von $s = 1$

$$f_0(s; 2; k, \alpha) \sim 2k^{-2}(s-1)^{-2}\sum_{m=1}^{k} 1 \sum_{r=1}^{j(m)} 1 = 2k^{-2}(s-1)^{-2}\sum_{m=1}^{k} j(m).$$

Hierbei ist $j(m)$, die Anzahl der mod. k inkongruenten Lösungen der Kongruenz $mx \equiv \alpha\,(\mathrm{mod.}\,k)$, gleich (m, k), falls letztere Zahl ein Teiler von α ist, sonst gleich 0. Es sei $(m, k) = v$, also $v|\alpha$, $m = rv$, also $\left(r, \frac{k}{v}\right) = 1$. Dann sind bei festem v genau $\varphi\left(\frac{k}{v}\right)$ Werte für r und somit für m zulässig, da ja $1 \leqq r = \frac{m}{v} \leqq \frac{k}{v}$ ist. Folg-

[9]) Ramanujan, Collected Papers, Cambridge 1927, S. 134.

[10]) H. Kober, a. a. O. [2]), II. Teil.

[11]) E. Landau, Über die Anzahl der Gitterpunkte in gewissen Bereichen. II, Göttinger Nachr. 1915, S. 2—6 und 27—28.

lich ist der Koeffizient für $\frac{1}{2}f_0$ im Falle $h=2$

$$= k^{-2}\sum_{\nu|\alpha,\nu|k}\nu\varphi\left(\frac{k}{\nu}\right) = k^{-2}\sum_{\nu|(\alpha,k)}\nu\varphi\left(\frac{k}{\nu}\right).$$

Er ist also wohl für beliebiges h eine $(h-1)$-fache Summe; bezeichnet man ihn mit $H(h;\alpha,k)$, so gilt

$$(5,1)\qquad H(h;\alpha,k) = \frac{1}{k^h}\sum_{\nu_{h-1}|(\alpha,k)}\nu_{h-1}\varphi\left(\frac{k}{\nu_{h-1}}\right)\sum_{\nu_{h-2}|\nu_{h-1}}\nu_{h-2}\varphi\left(\frac{k}{\nu_{h-2}}\right)\cdots\sum_{\nu_1|\nu_2}\nu_1\varphi\left(\frac{k}{\nu_1}\right)$$

$$= \frac{1}{k^h}\sum_{\nu_1|\nu_2|\cdots|\nu_{h-1}|(\alpha,k)}\prod_{r=1}^{h-1}\nu_r\varphi\left(\frac{k}{\nu_r}\right).$$

Wenn α und β denselben größten Teiler mit k gemeinsam haben, etwa δ, so wäre $H(h;\alpha,k)=H(h;\beta,k)=H(h;\delta,k)$, $\delta|k$. Es wäre

$$\tfrac{1}{2}f_0(s;h+1;k,\alpha)\sim k^{-1}\sum_{m=1}^{k}H(h;m,k)(s-1)^{-h}\sum_{r=1}^{j(m)}\frac{1}{s-1} = \frac{(s-1)^{-h-1}}{k}\sum_{m=1}^{k}H(h;m,k)\,j(m)$$

in der Umgebung der Stelle $s=1$ auf Grund von (4, 2), also der Koeffizient

$$H(h+1;\alpha,k) = \frac{1}{k}\sum_{\substack{m=1\\(m,k)|\alpha}}^{k}H(h;m,k)(m,k) = \frac{1}{k}\sum_{\substack{m=1\\(m,k)=\nu|(\alpha,k)}}^{k}H(h;\nu,k)\nu = \frac{1}{k}\sum_{\nu|(\alpha,k)}H(h;\nu,k)\,\nu\varphi\left(\frac{k}{\nu}\right).$$

Denn setzt man wieder $(m,k)=\nu$ und betrachtet irgendein bestimmtes $\nu|k$, so gibt es wieder $\varphi\left(\frac{k}{\nu}\right)$ zugehörige Werte von m. Ist nämlich wieder $m=r\nu$, also $\left(r,\frac{k}{\nu}\right)=1$, so kann r genau $\varphi\left(\frac{k}{\nu}\right)$ Werte annehmen, da $r\geqq 1$ und wegen $m\leqq k$ weiterhin $r\leqq\frac{k}{\nu}$ ist. Also erhält man für $H(h+1;\alpha,k)$ genau den $H(h;\alpha,k)$ in (5, 1) entsprechenden Ausdruck, q. e. d.

Es soll jetzt der Hauptkoeffizient der Funktion (s. (4, 6) u. (4, 4))

$$\tfrac{1}{2}G_0(s;h;k,\alpha,v) = \frac{1}{2}\sum_{\substack{n\equiv\alpha\,(\mathrm{mod.}\,k)\\n\neq 0}}\frac{d_h(|n|)}{|n|^s}e^{2i\pi vn} = \frac{1}{2}\sum_{r=0}^{l-1}e^{2i\pi v(\alpha+rk)}f_0(s;h;C,\alpha+rk);\quad v=\frac{a}{c},$$

bestimmt werden, und zwar nur in dem einfacheren Falle $(k,c)=1$, also $C=ck$, $l=c$. Er ist auf Grund des Vorhergehenden

$$(5,2)\qquad \sum_{r=0}^{c-1}e^{2i\pi v(\alpha+rk)}H(h;\alpha+rk,C) = C^{-h}\sum_{r=0}^{c-1}e^{2i\pi v(\alpha+rk)}\sum_{\nu_1|\nu_2|\cdots|\nu_{h-1}|(\alpha+rk,C)}\prod_{n=1}^{h-1}\nu_n\varphi\left(\frac{C}{\nu_n}\right).$$

Welche Werte von r gehören zu einem festen ν_{h-1}, einem beliebig angenommenen Teiler von C, der kurz ν heißen soll?

Es sei $\Delta=(\alpha,k)$. Damit die Kongruenz $\alpha+rk\equiv 0\,(\mathrm{mod.}\,\nu)$ eine Lösung r haben soll, muß $\delta=(k,\nu)|\alpha$, also auch $\delta|\Delta$ sein. Es ist $\left(\frac{k}{\delta},\frac{\nu}{\delta}\right)=1$, $\nu|C=ck$, also $\frac{\nu}{\delta}\Big|\frac{ck}{\delta}$, folglich $\frac{\nu}{\delta}\Big|c$. Es sei r_1 die kleinste nicht negative Lösung der Kongruenz, dann sind die zulässigen Lösungen

$$r_1,\ r_2=r_1+\frac{\nu}{\delta},\quad r_3=r_1+\frac{2\nu}{\delta},\ \ldots,\ r_j=r_1+(j-1)\frac{\nu}{\delta};\quad r_j\leqq c-1<r_{j+1}.$$

Folglich ist $j=c:\frac{\nu}{\delta}=\frac{c\delta}{\nu}$, da $0\leqq r_1<\frac{\nu}{\delta}$ ist, und wegen $v=\frac{a}{c}$ ist

$$(5,21)\qquad \sum_{m=1}^{\frac{c\delta}{\nu}} e^{2i\pi\nu(\alpha+r_m k)} = e^{2i\pi\nu(\alpha+r_1 k)} \sum_{n=0}^{j-1} e^{2i\pi\frac{\nu v k n}{\delta}} = e^{2i\pi\nu(\alpha+r_1 k)} \sum_{n=0}^{j-1} e^{2i\pi n\frac{ak}{j}}.$$

Nun ist die letzte Summe, da $j \mid c$, $(c, a) = 1$, $(c, k) = 1$, sicher gleich 0, außer für $j = 1$; dann ist sie ebenfalls gleich 1; für $j = 1$ ist $\nu = c\delta$, da aber $\alpha + r_1 k \equiv 0 \pmod{\nu}$, ist $c \mid (\alpha + r_1 k)$, $(\alpha + r_1 k)\nu$ ganz, also die ganze rechte Seite gleich 1. Es kommen daher für die Summen auf der rechten Seite von (5, 2) nur solche Teiler ν von $C = ck$ in Betracht, deren Form $\nu = c\delta$, $\delta \mid \Delta$ ist, und umgekehrt führt jeder Teiler δ von Δ zu einem solchen zulässigen ν, weil dann $(k, \nu) = (k, c\delta) = \delta \mid \Delta \mid \alpha$, also die Kongruenz $\alpha + rk \equiv 0 \pmod{\nu}$ lösbar ist. Folglich ist der gesuchte Koeffizient, da $\frac{C}{\nu} = \frac{k}{\delta}$ ist, gleich

$$(5,3)\qquad \frac{c}{C^h} \sum_{\substack{\nu_1 \mid \nu_2 \mid \cdots \mid \nu_{h-2} \mid c\delta \\ \delta \mid \Delta = (\alpha, k)}} \prod_{n=1}^{h-2} \nu_n \varphi\left(\frac{C}{\nu_n}\right) \delta \varphi\left(\frac{k}{\delta}\right) = \frac{c}{C^h} \sum_{\mu_1 \mid \mu_2 \mid \cdots \mid \mu_{h-2} \mid c} \prod_{n=1}^{h-2} \mu_n \varphi\left(\frac{c}{\mu_n}\right) \cdot \sum_{\tau_1 \mid \tau_2 \mid \cdots \mid \tau_{h-1} \mid (\alpha, k)} \prod_{n=1}^{h-1} \tau_n \varphi\left(\frac{k}{\tau_n}\right).$$

Die letzte Umformung ergibt sich z. B. im Falle $h = 3$ folgendermaßen:

$$\sum_{\nu_1 \mid c\delta, \delta \mid \Delta} \nu_1 \varphi\left(\frac{C}{\nu_1}\right) \delta \varphi\left(\frac{k}{\delta}\right) = \sum_{\substack{\mu \mid c \\ \tau \mid \delta \mid \Delta}} \mu\tau \varphi\left(\frac{c}{\mu} \; \frac{k}{\tau}\right) \delta \varphi\left(\frac{k}{\delta}\right) = \sum_{\substack{\mu \mid c \\ \tau \mid \delta \mid \Delta}} \mu \varphi\left(\frac{c}{\mu}\right) \cdot \tau \varphi\left(\frac{k}{\tau}\right) \cdot \delta \varphi\left(\frac{k}{\delta}\right)$$

$$= \sum_{\mu \mid c} \mu \varphi\left(\frac{c}{\mu}\right) \cdot \sum_{\tau \mid \delta \mid \Delta = (a, k)} \tau \varphi\left(\frac{k}{\tau}\right) \cdot \delta \varphi\left(\frac{k}{\delta}\right).$$

Man erhält nämlich alle Teiler ν_1 von $c\delta$, indem man $\nu_1 = \mu\tau$ setzt und μ alle Teiler von c, τ alle Teiler von δ durchlaufen läßt, weil $\delta \mid k$, $(c, k) = 1$, also $(c, \delta) = 1$ ist; ferner ist auch $\left(\frac{c}{\mu}, \frac{k}{\tau}\right) = 1$, also φ in ein Produkt aufspaltbar. Ganz entsprechend verfährt man durch Zerspaltung der weiter noch auftretenden Teiler ν im Falle $h > 3$. Im Falle $h = 2$ ist der Hauptkoeffizient von $\frac{1}{2}G_0$

$$(5,4)\qquad H(2; \alpha, k, v) = \frac{c}{C^2} \sum_{\tau \mid (\alpha, k)} \tau \varphi\left(\frac{k}{\tau}\right),$$

also

$$H(2; \alpha, k, v) = \frac{1}{c} \text{ für } k = 1 \text{ und allgemeiner } = cC^{-2}\varphi(k) \text{ für } (k, \alpha) = 1 = (k, c).$$

Aus (5, 3) ist sofort ersichtlich, daß der Hauptkoeffizient stets > 0 ist, daß also die Funktionen

$$G_0(s; h; k, \alpha, v) = \sum_{\substack{n \equiv \alpha \pmod{k} \\ n > 0}} d_h(n)\, n^{-s} e^{2i\pi v n} + \sum_{\substack{n \equiv -\alpha \pmod{k} \\ n > 0}} d_h(n)\, n^{-s} e^{-2\pi i v n},$$

und daher auch die Funktion $\sum_{0 < n \equiv \alpha}$, weil die Differenz der beiden Reihen gleich G_1 (s. (4, 6)) ganz ist, im Punkte $s = 1$ singulär sind für jedes rationale v, dessen Nenner teilerfremd zu k ist. Da aber diese v auf dem Einheitskreise dicht liegen, folgt aus Satz III:

Satz IV. *Es sei $h \geqq 2$, $k \geqq 1$ ganz, α beliebig ganz. Dann hat die Potenzreihe $\Sigma d_h(n) x^n$, in der n alle positiven ganzen Zahlen der Reihe $n \equiv \alpha \pmod{k}$ durchläuft, den Einheitskreis zur natürlichen Grenze.*

Dasselbe Ergebnis folgt natürlich aus der Singularität von G_0 im Punkte $s = 1$ für die Potenzreihe, in der n alle positiven ganzen Zahlen $\equiv \pm \alpha \pmod{k}$ durchläuft.

Es sei nun $(k, \alpha) = 1$, dann ist der Hauptkoeffizient nach (5, 3)

$$(5,5)\qquad = k^{-h}\varphi^{h-1}(k)\, E(h; c), \quad \text{wenn} \quad E(h; c) = c^{1-h} \sum_{\nu_1 \mid \nu_2 \mid \cdots \mid \nu_{h-2} \mid c} \prod_{1}^{h-2} \nu_n \varphi\left(\frac{c}{\nu_n}\right).$$

Es sollen jetzt schließlich noch einige einfache Eigenschaften von $E(h;c)$ dem Hauptkoeffizienten im Falle $k=1$, bewiesen werden; die letzte, (5, 8), wird im folgenden Abschnitt notwendig gebraucht.

Es sei für $n=1,2,\ldots,h-2$ jetzt $\nu_{h-n-1}\tau_n = c$, dann ist für $h \geqq 3$

$$(5,6) \qquad \tau_1 \mid \tau_2 \mid \ldots \mid \tau_{h-2} \mid c, \quad E(h;c) = \frac{1}{c} \sum_{\tau_1\mid\tau_2\mid\cdots\tau_{h-2}\mid c} \prod_{1}^{h-2} \frac{\varphi(\tau_n)}{\tau_n}$$

$$= \frac{1}{c} \sum_{\tau \mid c} \varphi(\tau)\, E(h-1;\tau)\,.$$

Denn es ist

$$\frac{1}{\tau_{h-2}} \sum_{\tau_1\mid\tau_2\mid\cdots\mid\tau_{h-2}} \prod_{1}^{h-3} \frac{\varphi(\tau_n)}{\tau_n} = E(h-1;\tau_{h-2})\,,$$

man schreibe statt τ_{h-2} nur τ und berücksichtige (5, 4) und $E(2;\tau) = \frac{1}{\tau}$.

Ferner: Es sei $c = ab$ und $(a,b)=1$, dann ist

$$(5,7) \qquad E(h;c) = E(h;a)\cdot E(h;b)\,.$$

Der Satz ist für $h=2$ richtig, er möge für h allgemein gelten, dann ist er auch für $h+1$ richtig. Denn wenn $\tau = \tau_1\tau_2$, $\tau_1 \mid a$, $\tau_2 \mid b$, ist nach (5, 6)

$$E(h+1;ab) = \frac{1}{ab} \sum_{\tau\mid ab} \varphi(\tau)\, E(h;\tau) = \frac{1}{ab} \sum_{\substack{\tau_1\mid a \\ \tau_2\mid b}} \varphi(\tau_1\tau_2)\, E(h;\tau_1\tau_2)$$

$$= \frac{1}{ab} \sum_{\tau_1\mid a} \varphi(\tau_1)\, E(h;\tau_1) \sum_{\tau_2\mid b} \varphi(\tau_2)\, E(h;\tau_2) = E(h+1;a)\cdot E(h+1;b)\,.$$

Schließlich gilt der Satz:

Es sei $c \mid C$ und $c < C$, d. h. c ein echter Teiler von C. Dann ist

$$(5,8) \qquad E(h;C) < E(h;c)\,.$$

Für $h=2$ ist dies nach (5, 4) richtig. Es möge für h stimmen. Es ist dann

$$E(h+1;c) = \frac{1}{c} \sum_{\tau\mid c} E(h;\tau)\,\varphi(\tau)\,.$$

Folglich ist für $c>1$ auf Grund der Annahme: $1 = E(h;1) \geqq E(h;\tau) \geqq E(h;c)$

$$\frac{1}{c} \sum_{\tau\mid c} E(h;1)\,\varphi(\tau) > E(h+1;c) > \frac{1}{c} \sum_{\tau\mid c} E(h;c)\,\varphi(\tau)\,,$$

also, da $\sum_{\tau\mid c} \varphi(\tau) = c$,

$$(5,81) \qquad 1 > E(h+1;c) > E(h;c);$$

für $c=1$ tritt Gleichheit ein.

Es genügt, die Richtigkeit des Satzes für $h+1$ im Falle $C = cp$, p Primzahl, zu beweisen. Es sei also

$$c = p^\alpha Q, \quad C = p^{\alpha+1}Q, \quad \alpha \geqq 0, \quad (p,Q) = 1\,.$$

Dann braucht man auf Grund von (5, 7) nur noch zu zeigen, daß

$$E(h+1;p^{\alpha+1}) < E(h+1;p^\alpha)$$

ist. Nach (5, 6) ist

$$E(h+1;p^{\alpha+1}) = p^{-\alpha-1}\{\sum_{\tau\mid p^\alpha} \varphi(\tau)\, E(h;\tau) + \varphi(p^{\alpha+1})\, E(h;p^{\alpha+1})\}$$

$$= \frac{1}{p}\, E(h+1;p^\alpha) + \frac{p-1}{p}\, E(h;p^{\alpha+1})\,,$$

$$E(h+1;p^\alpha) - E(h+1;p^{\alpha+1}) = \frac{p-1}{p}\{E(h+1;p^\alpha) - E(h;p^{\alpha+1})\},$$

und hier ist die rechte Seite nach (5, 81) positiv, da nach der Annahme

$$E(h; p^{\alpha+1}) < E(h; p^{\alpha})$$

sein soll. So ist der Satz (5, 8) bewiesen.

6. Die Reihen $\Sigma d_h(n) x^n \cos 2\pi vn$, $\Sigma d_h(n) x^n \sin 2\pi vn$.

A. *Es sei* $2v = \frac{\nu}{m}$, $m > 1$, $(2\nu, m) = 1$; *dann gibt es eine über den Einheitskreis nicht fortsetzbare Funktion* $\Sigma a_n x^n$, *während die Funktion* $\Sigma a_n x^n \cos 2\pi vn$ *über den Kreis hinaus fortsetzbar ist.*

1. Es sei

$$f(x) = \sum_{n=1}^{\infty} n^{-4} \sum_{-\frac{n}{m} < r < \frac{n}{m}, (r,n)=1} (x - e^{\pi i \frac{r}{n}})^{-1}.$$

Auf dem Einheitskreise ist $x = e^{i\varphi}$, es sei $-\pi \leqq \varphi < \pi$. In jedem Punkte des Bogens $-\frac{\pi}{m} \leqq \varphi \leqq \frac{\pi}{m}$ dieses Kreises ist nun $f(x)$ singulär, in der ganzen übrigen Ebene aber regulär. Zuerst wird die letzte Behauptung bewiesen. Man umgebe den Singularitätsbogen mit der geschlossenen Kurve, deren jeder Punkt von dem bezüglich nächsten Punkte des Bogens den Abstand δ hat, $0 < \delta < \frac{1}{2}$. Schließt man das Innere dieser Kurve von der Ebene aus, so ist

$$\left| x - \exp\left(\frac{\pi i r}{n}\right) \right| \geqq \delta .$$

Die Anzahl der Glieder der inneren Summe der Doppelreihe, die $f(x)$ darstellt, ist $\leqq 2\varphi(n)$, und $\Sigma \varphi(n) n^{-4}$ konvergiert, also konvergiert die Doppelreihe in diesem Gebiete absolut und gleichmäßig und stellt eine reguläre Funktion dar.

Es seien nun a und b ganz, $(a, b) = 1$, $-\frac{1}{m} < \frac{a}{b} < \frac{1}{m}$, also $x_0 = \exp\left(\frac{\pi i a}{b}\right)$ ein Punkt des Bogens $-\frac{\pi}{m} \leqq \varphi \leqq \frac{\pi}{m}$ des Einheitskreises. Dann ist für alle ganzen r, n, wenn $(r, n) = 1$, bis auf eine Menge I endlich vieler Wertepaare, sicher $\left| \frac{a}{b} - \frac{r}{n} \right| > n^{-2}$, die Menge der letzteren Wertepaare sei II; I′ und II′ seien bezüglich die Teilmengen der Wertepaare, für die $\left| \frac{r}{n} \right| < \frac{1}{m}$ ist. Es sei nun $\varrho \geqq 0$, dann ist für die Menge II′

$$\frac{1}{n^2} < \left| \frac{a}{b} - \frac{r}{n} \right|, \quad \pi \left| \frac{a}{b} - \frac{r}{n} \right| < \frac{2\pi}{m} \leqq \frac{2\pi}{3},$$

$$\left| \varrho x_0 - \exp\left(\frac{\pi i r}{n}\right) \right|^2 \geqq (\varrho - 1)^2 + 4\varrho \sin^2\left(\frac{a\pi}{2b} - \frac{r\pi}{2n}\right) \geqq \sin^2\left(\frac{a\pi}{b} - \frac{r\pi}{n}\right) > \frac{1}{2n^4}.$$

Daher konvergiert die Reihe $\sum_{\text{II}'}$ in

$$f(x) = \sum_{\text{I}'} + \sum_{\text{II}'}$$

gleichmäßig in ϱ für $x = \varrho x_0$; die Reihe $\sum_{\text{I}'}$ aber besteht nur aus endlich vielen Gliedern, alle Glieder sind stetige Funktionen von ϱ bis auf das eine $n = b$, $r = a$, das für $\varrho \to 1$ unendlich groß wird. Also wird $f(x)$ für $\varrho \to 1$ unendlich groß; da $\frac{a}{b}$ jeder Bruch des Intervalles $\left(-\frac{1}{m}, \frac{1}{m}\right)$ sein kann, ist $f(x)$ in jedem Punkte des Bogens $-\frac{\pi}{m} \leqq \varphi \leqq \frac{\pi}{m}$ des Einheitskreises singulär. — Für $|x| < 1$ ist also $f(x) = \sum_{n=0}^{\infty} b_n x^n$.

2. Es mögen v, ν, m die oben festgelegte Bedeutung haben, also m ungerade sein, ferner sei $a_n = \dfrac{b_n}{\cos 2\pi vn}$ und $F(x) = \Sigma a_n x^n$, also $f(x) = \Sigma a_n \cos(2\pi n v)\, x^n$. Es ist

$$(6,1) \qquad \frac{1}{\cos 2\pi nv} = \frac{1}{\cos \pi n \dfrac{\nu}{m}} = \sum_{k=0}^{m-1} (-1)^k e^{-(2k+1)i\pi \frac{n\nu}{m}},$$

also für $|x| < 1$

$$(6,2) \qquad F(x) = \sum_{n=0}^{\infty} \frac{b_n}{\cos 2\pi nv}\, x^n = \sum_{k=0}^{m-1} (-1)^k f\left(xe^{-(2k+1)i\pi \frac{\nu}{m}}\right).$$

Da $f(x)$ in jedem Punkte des Bogens $-\dfrac{\pi}{m} \leqq \arg x \leqq \dfrac{\pi}{m}$ des Einheitskreises singulär, in jedem anderen Punkte des Kreises aber regulär ist, so ist die ebenfalls eindeutige Funktion $f_k(x) = f\left(xe^{-(2k+1)i\frac{\pi\nu}{m}}\right)$ auf dem Bogen des Einheitskreises

$$\frac{\pi}{m}\{-1 + \nu(2k+1)\} \leqq \arg x \leqq \frac{\pi}{m}\{1 + \nu(2k+1)\}$$

singulär, auf dem ganzen übrigen Kreise aber regulär. Da aber diese Singularitätsbögen für $k = 0, 1, 2, \ldots, m-1$ genau die Gesamtlänge 2π haben und sich der Bogen, der zu k' gehört, an den Bogen k genau im positiven Sinne anschließt, für den

$1 + \nu(2k+1) = -1 + \nu(2k'+1) + 2m \cdot$ ganze Zahl, also $\nu(k'-k) - 1 \equiv 0 \pmod m$

ist — die Kongruenz hat stets eine Lösung $0 \leqq k' < m$, $k' \neq k$ —, so findet keine Überdeckung statt. Jeder Punkt x des Einheitskreises, bis auf die m Teilpunkte, gehört genau einem (s. (6, 2)) Singularitätsbogen an. Folglich hat $F(x)$ den Kreis zur natürlichen Grenze, während $f(x)$ über den Kreis fortsetzbar ist.

Ganz entsprechend läßt sich ein Gegenbeispiel konstruieren für den Fall $F_1(x) = \Sigma a_n' x^n$, $f_1(x) = \Sigma a_n' x^n \sin 2\pi vn = f(x) - f(-x)$, wenn $2v = \dfrac{\nu}{m}$, $(\nu, m) = 1$ und $m \geqq 4$ gerade ist, auf Grund von

$$(6,3) \qquad \sum_{k=0}^{\frac{m}{2}-1} e^{-2\pi i k n \frac{\nu}{m}} = \frac{e^{2i\pi vn}}{i \sin 2\pi vn}$$

für ungerades n, also, da $f_1(x) = f(x) - f(-x)$ ungerade ist,

$$(6,4) \qquad F_1(x) = \sum_{n>0,\ \text{ungerade}} \frac{2b_n}{\sin 2\pi nv}\, x^n = i \sum_{k=0}^{\frac{m}{2}-1} f_1\left(xe^{-(2k+1)i\frac{\nu\pi}{m}}\right).$$

$f_1(x)$ ist in der Ebene bis auf die beiden Singularitätsbögen des Einheitskreises $-\dfrac{\pi}{m} \leqq \arg x \leqq \dfrac{\pi}{m}$, $\pi\left(1 - \dfrac{1}{m}\right) \leqq \arg x \leqq \pi\left(1 + \dfrac{1}{m}\right)$ regulär, also ebenso

$$f_1\left(x \exp\left\{-(2k+1)\frac{i\pi\nu}{m}\right\}\right)$$

bis auf die Bögen:

$$\frac{\pi}{m}(-1 + \nu(2k+1)) \leqq \arg x \leqq \frac{\pi}{m}(1 + \nu(2k+1)),$$

$$\frac{\pi}{m}(m - 1 + \nu(2k+1)) \leqq \arg x \leqq \frac{\pi}{m}(m + 1 + \nu(2k+1)).$$

Da sich hier wieder sämtliche $2 \cdot \frac{m}{2} = m$ Singularitätsbögen zum vollen Kreis lückenlos aneinanderschließen, ist $F_1(x)$ über den Einheitskreis nicht fortsetzbar. — Ähnlich, nur einfacher, kann man ein Gegenbeispiel für den umgekehrten Fall bilden.

B. *Die Reihe* $\sum_{n=1}^{\infty} d_h(n)\, x^n \cos 2\pi nv$ *für rationale* v, $h \geqq 2$.

Es sei v rational fest, v' rational,

$$G(s; v') = \sum_{n=1}^{\infty} d_h(n)\, n^{-s} e^{2\pi i v' n} \cos 2\pi vn = G_2(s; v') + iG_3(s; v'),$$

$$G_{\frac{2}{3}}(s; v') = \sum_{n=1}^{\infty} d_h(n) n^{-s} \cos 2\pi vn \begin{cases} \cos 2\pi v'n \\ \sin 2\pi v'n \end{cases}.$$

Nun ist aber $2 \cos 2\pi vn \cdot \cos 2\pi v'n = \cos 2\pi (v + v')n + \cos 2\pi (v - v')n$, der Hauptkoeffizient der Funktion $\frac{1}{2} G_0(s; h; 1, 0, v \pm v') = \sum_{n=1}^{\infty} d_h(n)\, n^{-s} \cos 2\pi (v \pm v')n$ ist, wenn N_2 bzw. N_1 die Nenner der Brüche $v \pm v'$ bedeuten, nach (5, 5) gleich $E(h; N_2)$ bzw. $E(h; N_1)$, also positiv.

Folglich hat $G_2(s; v')$ einen positiven, $G(s; v')$ einen von 0 verschiedenen Hauptkoeffizienten, wie man durch Beschränkung auf reelles s erkennt. $G(s; v')$ hat daher in $s = 1$ eine Singularität, und die zu untersuchende Reihe hat nach Satz III den Einheitskreis zur natürlichen Grenze.

C. *Die Reihe* $\sum_{n=1}^{\infty} d_h(n)\, x^n \sin 2\pi nv$ *für rationales* v, $h \geqq 2$.

Es ist $v = \frac{a}{c}$, $(a, c) = 1$, $c > 2$, da sonst die Reihe identisch 0 ist. Da $2\Im(e^{2i\pi v' n} \sin 2\pi vn) = \cos 2n\pi (v - v') - \cos 2n\pi (v + v')$, so braucht man nur zu beweisen, daß (s. (4, 4)) die Funktionen

$$F_0(s; h; 1, 0, v + v') \quad \text{und} \quad F_0(s; h; 1, 0, v - v')$$

verschiedene Hauptkoeffizienten haben. Dann kann man daraus folgern, daß $\Im(\Sigma d_h(n)\, n^{-s} e^{2\pi i n v'} \sin 2\pi vn)$, für reelles s gebildet, einen von 0 verschiedenen reellen Hauptkoeffizienten hat, die Funktion also eine Singularität in $s = 1$ besitzt, u. s. f.

Die Hauptkoeffizienten von $F_0(\ldots, v + v')$ und $F_0(\ldots, v - v')$ sind nun nach (5, 5) gleich $2E(h; N_2)$ bzw. $2E(h; N_1)$, wenn N_1 bzw. N_2 die Nenner der rationalen Zahlen $v - v'$, $v + v'$ sind. Wenn man nun zeigen kann, daß für eine überall dichte Menge gewisser rationaler v' stets $N_2 \mid N_1$, $N_2 < N_1$ ist, so folgt dann aus Satz (5, 8) $E(h; N_1) < E(h; N_2)$ und alles andere.

Es sei also y eine beliebige, feste reelle Zahl, $\delta > 0$ beliebig gegeben, dann gibt es stets ein rationales v' so, daß $|y - v'| \leqq \delta$ und $N_2 \mid N_1$, $N_2 < N_1$ ist, wenn $c > 2$ und N_2, N_1 die Nenner der gekürzten Brüche $(v \pm v')$ sind: Man bringe c in eine Form

$$c = rQ, Q = q^{\alpha} \text{ eine Primzahlpotenz}, \quad (q, r) = 1.$$

Es sei p eine Primzahl $> 2c$ und so groß, daß $N = pc > \frac{2c + 1}{2\delta}$ ist. Dann liegen im Intervall $\langle y - \delta, y + \delta \rangle$ mindestens $2c$ Brüche, deren Nenner gleich N ist und deren Zähler sich um je 1 unterscheiden. Die Zähler seien $C_1, C_2, \ldots, C_{2c}$, wobei $C_{\nu+1} = C_\nu + 1$ sei; es gibt darunter $2r = 2c : Q$ von der Art, daß bei dem Bruche

$$\frac{C_\nu + ap}{N} = \frac{C_\nu}{N} + \frac{ap}{N} = \frac{C_\nu}{N} + v$$

der Zähler $C'_\nu = C_\nu + ap$ durch Q teilbar ist. Sie seien C_μ, $C_\mu + Q, \ldots, C_\mu + (2r-1)Q$. In der ersten Hälfte dieser Zahlenreihe etwa sei jede Zahl durch p unteilbar; sonst ist das bei der zweiten Hälfte der Fall, da $p > 2c = 2rQ > C_{2c} - C_1$. Unter diesen r Zahlen $C_\mu, C_\mu + Q, \ldots, C_\mu + (r-1)Q$ gibt es mindestens eine, C', für welche $C' - ap$ zu r teilerfremd ist, da $(Q, r) = 1$. Dann ist also $C' - ap$ teilerfremd zu p, r; $C' + ap$ ist durch Q teilbar, daher, falls Q ungerade ist, $C' - ap = C' + ap - 2ap$ wegen $(a, c) = 1$, also $(a, Q) = 1$ und $p > 2c = 2rQ$, zu Q teilerfremd, also ist für $v' = \frac{C'}{N}$, der Bruch

$$v' - v = \frac{C'}{N} - \frac{a}{c} = \frac{C' - ap}{rpQ} \text{ nicht kürzbar, } v' + v = \frac{C' + ap}{rpQ}$$

aber mindestens durch Q kürzbar, also $N_2 | N_1$ und $N_2 < N_1$.

Falls aber Q gerade und $r = 1$, so ist $Q = 2^\alpha$, $\alpha > 1$, $C' + ap$ also mindestens durch 4 teilbar, $C' - ap = C' + ap - 2ap$ aber, da ap ungerade ist, $\equiv 2 \pmod 4$, also ist $N_1 = \frac{cp}{2}$, $N_2 | N_1$ und $< N_1$, q. e. d.

D. *Der Fall eines irrationalen v für $h = 2$.* Dann muß man, entsprechend wie im Falle B und C, beweisen, daß die beiden Funktionen

$$\sum_1^\infty \frac{d(n)}{n^s} (\cos 2\pi n(v' - v) \pm \cos 2\pi n(v' + v)) = \sum_1^\infty \frac{d(n) A_n}{n^s}$$

für eine überall dichte Menge reeller v' je im Punkte $s = 1$ singulär sind.

Es sei v' irrational so gewählt, daß $v' - v = y$ rational ist; dann ist $v' + v = u$ irrational; diese v' liegen überall dicht.

Nun ist [12])

$$\sum_1^x d(n) \cos 2\pi n y = \frac{1}{N} x \log x + \boldsymbol{O}(x),$$

wenn N den Nenner des nicht mehr kürzbaren Bruches y bedeutet,

$$\sum_1^x d(n) \cos 2\pi n u = \boldsymbol{o}(x \log x)\,[13]), \quad \text{also}$$

$$B_x = \sum_1^x d(n) A_n = \frac{1}{N} x \log x \,(1 + \boldsymbol{o}(1)) > \alpha x \log x \quad \text{für} \quad \alpha = \frac{1}{2N}, \quad x \geqq A.$$

Hieraus aber läßt sich leicht für reelles $s > 1$ folgern:

$$\lim_{s=1} \sum_1^\infty \frac{d(n) A_n}{n^s} = \infty, \text{ d. h. } f(s) = \sum_1^\infty \frac{d(n) A_n}{n^s}$$

ist im Punkte $s = 1$ singulär. Also hat für irrationales v jede der beiden Funktionen $\sum_1^\infty d(n) x^n \begin{cases} \cos 2\pi vn \\ \sin 2\pi vn \end{cases}$ den Einheitskreis zur natürlichen Grenze. —

Ganz entsprechende Resultate lassen sich für die Reihen

$$\Sigma d_h(n) x^n \log^r n, \quad \Sigma d_h(n) x^n \log^r n \begin{cases} \cos \\ \sin \end{cases} 2\pi vn, \quad h \geqq 2,$$

für beliebiges ganzzahliges r herleiten, indem man mit den Ableitungen bzw. Integralen der Dirichletschen Reihen arbeitet, für irrationales v nur im Falle $h = 2$. Ebenso lassen sich die Resultate dieses Abschnittes insbesondere auch auf die entsprechenden Potenz-

[12]) Wilton, a. a. O. [1]), Gleichung (15 VI). — H. Kober, a. a. O. [2]), Einleitung.

[13]) Chowla, Walfisz, Wilton, a. a. O. [1]).

reihen $\Sigma a_n x^n$ ausdehnen, in denen n die Glieder einer arithmetischen Reihe durchläuft; beim Beweise des dem Fall C entsprechenden Ergebnisses z. B. braucht man nur p teilerfremd zur Differenz der Reihe anzunehmen unter Berücksichtigung von (5, 3). Nur der Fall D kann nicht verallgemeinert werden.

7. Die Erweiterung des Franelschen Kriteriums.

Es sei $c > 1$ ganz, jede der c Reihen $\sum_{n=1}^{\infty} \frac{b_{cn+l}}{(cn+l)^s}$, $l = 0, 1, 2, \ldots, c-1$, möge für $\sigma > 1$ konvergieren und daher auch die Reihe

$$F(x) = \sum_{n=1}^{\infty} \frac{b_n x^n}{1-x^n} = \sum_{m=1}^{\infty} a_m x^m \quad \text{mit} \quad a_m = \sum_{d|m} b_d$$

im Inneren des Einheitskreises konvergieren. Es existiere eine reelle Zahl ϱ so, daß für $s > 1$ (d. h. bei Annäherung von rechts durch reelles s)

$$\lim_{s\to 1} (s-1)^{\varrho} \sum_{n=0}^{\infty} \frac{b_{cn+l}}{(cn+l)^s} = 0 \text{ für } l = 1, 2, \ldots, c\,,$$

$$\lim_{s\to 1} (s-1)^{\varrho-1} \sum_{n=1}^{\infty} \frac{b_{cn}}{n^s} = A$$

ist, wobei A auch ∞ sein darf. Dann ist, wenn $(a, c) = 1$, $v = \frac{a}{c}$ ist, für $s > 1$

$$\lim_{s\to 1} (s-1)^{\varrho} \sum_{n=1}^{\infty} \frac{a_n e^{2\pi i n v}}{n^s} = \frac{A}{c}\,.$$

Fügt man den Voraussetzungen dieses Satzes noch $\varrho > 0$, $A \neq 0$ hinzu, so folgt sofort, daß $s = 1$ ein singulärer Punkt von $f(s; v) = \sum_{n=1}^{\infty} a_n n^{-s} e^{2\pi i n v}$ und daß also, mit Rücksicht auf Satz III, jede primitive c-te Einheitswurzel eine singuläre Stelle von $F(x)$ ist. Die zwei Teile der Voraussetzung,

$$(s-1)^{\varrho-1} \sum_{n=1}^{\infty} b_{nc} n^{-s} \to A \quad \text{und} \quad A \neq 0,$$

können dann durch die eine schwächere Bestimmung ersetzt werden:

$$(s-1)^{\varrho-1} \sum_{n=1}^{\infty} b_{nc} n^{-s} = \Omega(1) \quad \text{für} \quad s \to 1\,.$$

Aus diesem Singularitäts-Kriterium folgt sofort das Franelsche als ein Spezialfall für $\varrho = 1$ mit Hilfe des Abelschen Stetigkeitssatzes [14]) für Dirichletsche Reihen.

Es erfaßt auch den Fall $a_m = \sigma_u(m)$ für rein imaginäres u (s. Einleitung); man setze $\varrho = 1$, dann wird $A = c^u \zeta(1-u) \neq 0$.

Es erfaßt ebenso den Fall $a_m = d(m)$, also $b_n = 1$. Es sei $1 < \varrho \leqq 2$, ϱ sonst beliebig. Dann ist für $s > 1$, $s \to 1$

$$(s-1)^{\varrho} \sum_{n=0}^{\infty} \frac{b_{cn+l}}{(cn+l)^s} < (s-1)^{\varrho} \zeta(s) \to 0; \quad (s-1)^{\varrho-1} \sum \frac{b_{cn}}{n^s} = (s-1)^{\varrho-1} \zeta(s) = \Omega(1)\,.$$

Beweis des Satzes. $g(s; \alpha)$, G, G_1 mögen ganze Funktionen von s bedeuten. Die Reihe $f(s; v)$ konvergiert für $\sigma > 1$ [15]); denn

[14]) Landau, a. a. O. [7]), § 209.

[15]) Landau, a. a. O. [7]), § 213.

$$(7,1)\quad f(s;v)=\sum_{k=0}^{c-1}e^{2i\pi k\frac{a}{c}}\sum_{0<n\equiv k\,(\mathrm{mod.}\,c)}\frac{a_n}{n^s}=\sum_{k=0}^{c-1}e^{2i\pi k\frac{a}{c}}f(s;k,c)\,,$$

$$(7,2)\quad f(s;k,c)=\sum_{m=1}^{c}\sum_{\substack{n\equiv m\,(\mathrm{mod.}\,c)\\ n>0}}\frac{b_n}{n^s}\sum_{r=1}^{j(m)}\sum_{\substack{\tau\equiv m_r'(m)\\ \tau>0}}\tau^{-s}=c^{-s}\sum_{m=1}^{c}\sum_{n=0}^{\infty}\frac{b_{cn+m}}{(cn+m)^s}\sum_{r=1}^{j(m)}\zeta\left(s;\frac{m_r'}{c}\right).$$

Hier ist $j(m)$ wieder die Anzahl der Lösungen z der Kongruenz $mz\equiv k\,(\mathrm{mod.}\,c)$, m_r' durchläuft alle Lösungen z, $1\leqq m_r'\leqq c$. Nun ist

$$\zeta\left(s;\frac{m_r'}{c}\right)=\frac{1}{s-1}+g\left(s;\frac{m_r'}{c}\right),$$

$$(7,3)\quad f(s;k,c)=\frac{c^{-s}}{s-1}\sum_{m=1}^{c}j(m)\sum_{n=0}^{\infty}\frac{b_{cn+m}}{(cn+m)^s}+\sum_{m=1}^{c}G(s;m,k)\sum_{n=0}^{\infty}\frac{b_{cn+m}}{(cn+m)^s}.$$

Man setze die letzte unendliche Reihe $=\psi(s;m)$. Es ist

$$(7,4)\quad \sum_{k=0}^{c-1}e^{2\pi ik\frac{a}{c}}\sum_{m=1}^{c}j(m)\,\psi(s;m)=\sum_{m=1}^{c}\psi(s;m)\sum_{k=0}^{c-1}e^{2\pi ik\frac{a}{c}}j(m;k).$$

j hängt ja auch von k ab, es ist $j(m;k)=(m,c)$, falls $(m,c)\,|\,k$, andernfalls $=0$. Es sei $(m,c)=\delta$ und $k=\delta k'$, dann ist

$$\sum_{k=0}^{c-1}e^{2\pi ia\frac{k}{c}}j(m;k)=\delta\sum_{\delta|k,\,k=0}^{c-1}e^{2\pi ia\frac{k'}{c:\delta}}=\delta\sum_{k'=0}^{\frac{c}{\delta}-1}e^{2\pi ia\frac{k'}{c:\delta}}.$$

Diese Summe ist gleich c für $\delta=c$, dagegen 0 für alle anderen Teiler δ von c. Da nun, falls $(m,c)=\delta=c$, auch $m=c$ sein muß, ist nach (7, 1), (7, 3) und (7, 4)

$$\begin{aligned}f(s;v)&=\frac{c^{1-s}}{s-1}\,\psi(s;c)+\sum_{m=1}^{c}G_1(s;m)\sum_{n=0}^{\infty}\frac{b_{cn+m}}{(cn+m)^s}\\&=\frac{c^{1-2s}}{s-1}\sum_{n=1}^{\infty}\frac{b_{cn}}{n^s}+\sum_{m=1}^{c}G_1(s;m)\sum_{n=0}^{\infty}\frac{b_{cn+m}}{(cn+m)^s}.\end{aligned}$$

Nach Multiplikation mit $(s-1)^\varrho$ folgt für $s\to 1$

$$f(s;v)\,(s-1)^\varrho=c^{1-2s}\,(s-1)^{\varrho-1}\sum_{n=1}^{\infty}\frac{b_{cn}}{n^s}+o(1)\to\frac{A}{c},\ \text{q. e. d.}$$

Falls aber vorausgesetzt war:

$$(s-1)^{\varrho-1}\sum_{n=1}^{\infty}\frac{b_{nc}}{n^s}=\Omega(1),$$

folgt:

$$f(s;v)\,(s-1)^\varrho=\Omega(1),$$

und hieraus schließt man für $\varrho>0$, ebenso wie im vorigen Falle für $\varrho>0$, $A\neq 0$, daß $s=1$ eine singuläre Stelle von $f(s;v)$ ist, daß daher jede primitive c-te Einheitswurzel eine singuläre Stelle von $F(x)=\sum_{n=1}^{\infty}a_n x^n$ ist.

Eingegangen 1. Juli 1935.

Die Geometrie des linearen Strahlenkomplexes
gegründet auf seine Polarentheorie.

Von *G. Haenzel* in Karlsruhe.

In der Geometrie des Strahlenraumes spielt der lineare Strahlenkomplex eine ähnliche Rolle wie die Fläche zweiter Ordnung und Klasse in der Geometrie des Punkte- und Ebenenraumes. Daraus ergibt sich die Frage nach der Existenz einer durch den linearen Strahlenkomplex bestimmten polaren Korrelation, die der polaren Korrelation der Fläche zweiter Ordnung und Klasse im Punkte- und Ebenenraum entspricht. Vielfach glaubt man im Nullraume des linearen Strahlenkomplexes die Analogie zum polaren Raume der Fläche zweiter Ordnung zu sehen. Diese Auffassung ist unberechtigt. Einmal ist der lineare Strahlenkomplex nicht das Inzidenzgebilde seines Nullraumes in dem Sinne wie die Fläche zweiter Ordnung die Inzidenzfläche ihres polaren Raumes darstellt; außerdem werden im Nullraume Punkt und Ebene als Elemente einander zugeordnet, während doch in einer polaren Korrelation der Strahlengeometrie nur Strahlengebilde als Pol und Polargebilde einander gegenübertreten müßten. Deutet man endlich die Linienkoordinaten als Punkte eines Hyperraumes, so erscheint die Korrelation des Nullraumes überhaupt als involutorische Perspektivität in diesem Hyperraume. Nun bedingt der lineare Strahlenkomplex wirklich eine polare Korrelation im Strahlenraume, und zwar als ihr Inzidenzgebilde. Die Grundlagen dieser Polarität werden im folgenden zuerst entwickelt.

In den weiteren Abschnitten kommt eine Abbildung des linearen Strahlenkomplexes auf den dreidimensionalen Punkteraum zur Anwendung, auf die zuerst M. Noether[1]) algebraisch hingewiesen hat. Sie wurde später von S. Lie sowie von F. Klein zur Formulierung und zum Beweise mancher liniengeometrischen Theoreme benutzt. Die Noethersche Abbildung liefert nicht nur eine Isomorphie zu der in unserem ersten Abschnitt abgeleiteten Polarentheorie, sondern ihre weitere Ausgestaltung ermöglicht eine einfache Darstellung bekannter und neuer Theoreme über die Geometrie der im linearen Strahlenkomplexe enthaltenen Strahlenkongruenzen und Regelscharen. Im Anschluß an die aufgestellte Polarentheorie des linearen Komplexes ergibt sich die bisher unbekannte Theorie seiner Involutionen und seiner involutorisch selbstgescharten Kongruenzen und Regelscharen. Eine weitere Arbeit über die Geometrie des linearen Komplexes soll sich hier anschließen.

I. Die Polarentheorie des linearen Strahlenkomplexes.

1. Ausgehend von den Plückerschen Linienkoordinaten

$$p_{ik} = x_i y_k - x_k y_i \qquad (i, k = 1, \ldots, 4)$$

[1]) M. Noether, Zur Theorie der algebraischen Funktionen mehrerer komplexen Variablen, Nachr. d. Kgl. Ges d. Wissenschaften zu Göttingen 1869, Nr. 15.

einer gegebenen Geraden XY werden durch die linearen Substitutionen

$$\varrho p_1 = p_{12} + p_{34}, \qquad \varrho p_3 = (p_{13} + p_{42}), \qquad \varrho p_5 = (p_{14} - p_{23}),$$
$$\varrho p_2 = i(p_{34} - p_{12}), \qquad \varrho p_4 = i(p_{42} - p_{13}), \qquad \varrho p_6 = (p_{14} + p_{23})$$

die sechs neuen Linienkoordiaten $p_i (i = 1, \ldots, 6)$ eingeführt. Die Plückersche Fundamentalrelation zwischen den Linienkoordinaten hat dann die Form:

$$P^2 = p_1^2 + p_2^2 + p_3^2 + p_4^2 - p_5^2 + p_6^2 = 0\,.$$

Die Invariante eines gegebenen linearen Strahlenkomplexes mit der Gleichung $\Sigma_1^6 a_i p_i = 0$ schreibt sich:

$$(\alpha)^2 = a_1^2 + a_2^2 + a_3^2 + a_4^2 - a_5^2 + a_6^2\,.$$

Die simultane Invariante zweier linearen Strahlenkomplexe mit den Gleichungen $\Sigma a_i p_i = 0$ und $\Sigma b_i p_i = 0$ lautet:

$$(\alpha\beta) = a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4 - a_5 b_5 + a_6 b_6\,.$$

Die sechs Gleichungen

$$p_i = 0 \qquad (i = 1, 2, \ldots, 6)$$

stellen sechs Fundamentalkomplexe[2]) dar, deren ursprüngliche Gleichungen aus den obigen Substitutionen folgen. Jeder von ihnen ist für die fünf übrigen nullinvariant. Je vier Fundamentalkomplexe haben zwei (reelle oder konjugiert imaginäre) windschiefe Strahlen gemein, die Leitgeraden der Schnittkongruenz der beiden übrigen Fundamentalkomplexe. So gehen die vier linearen Strahlenkomplexe mit den Gleichungen

$$p_i = 0 \qquad (i = 1, \ldots, 4)$$

durch die Geraden

$$u: \qquad x_1 = x_4 = 0$$

und

$$v: \qquad x_2 = x_3 = 0\,.$$

Die lineare Strahlenkongruenz C_v^u mit den Leitgeraden u, v ist dargestellt durch

$$p_{14} = p_{23} = 0 \text{ oder durch } p_5 = p_6 = 0.$$

Ein gegebener linearer Strahlenkomplex kann bei geeigneter Wahl des Koordinatentetraeders stets durch

$$p_6 = p_{14} + p_{23} = 0$$

wiedergegeben werden.

2. Der gegebene lineare Strahlenkomplex Γ mit der Gleichung $p_6 = 0$ enthält ∞^4 lineare Kongruenzen; sie bilden eine lineare Mannigfaltigkeit vierter Stufe, den C_1^1-*Raum* des Komplexes Γ. Für den Komplex Γ sind ∞^4 lineare Strahlenkomplexe nullinvariant; sie bilden gleichfalls eine lineare Mannigfaltigkeit vierter Stufe, den Γ_0-*Raum* des Komplexes Γ. Die Gleichung

$$\Sigma_1^5 \lambda_i p_i = 0$$

zwischen den Linienkoordinaten und den Parametern λ_i hat unter diesen Umständen eine doppelte geometrische Bedeutung: Für jedes Verhältnis der λ_i stellt sie eine in Γ enthaltene lineare Strahlenkongruenz und einen für Γ nullinvarianten linearen Komplex dar. Dabei geht dieser Komplex immer durch jene Kongruenz. Die obige Gleichung kennzeichnet also gleichzeitig das Element des C_1^1-Raumes und das Element des Γ_0-Raumes

[2]) F. Klein, Zur Theorie der Linienkomplexe des ersten und zweiten Grades, Math. Annalen **2** (1870).

des linearen Komplexes Γ. Beide Räume sind zueinander perspektiv. Der C_1^1-Raum enthält ∞^4 hyperbolische und ∞^4 elliptische lineare Kongruenzen; ihre Leitgeraden sind je zwei im Nullraume von Γ einander zugeordnete Strahlen. Der C_1^1-Raum enthält ∞^3 parabolische lineare Kongruenzen, deren je vereinigte Leitgeraden mit je einem Komplexstrahle von Γ zusammenfallen. Die Parameterwerte λ_i der parabolischen Kongruenzen unterliegen der Bedingungsgleichung:

$$\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2 - \lambda_5^2 = 0\,.$$

Gleichzeitig kennzeichnet diese Gleichung im Γ_0-Raum von Γ die ∞^3 speziellen linearen Komplexe, deren Achsen die Leitgeraden jener ∞^3 parabolischen Kongruenzen sind.

Zwei lineare Komplexe des Γ_0-Raumes und die beiden mit ihnen inzidenten linearen Kongruenzen des C_1^1-Raumes von Γ mit den Gleichungen $\Sigma_1^5 a_i p_i = 0$, $\Sigma_1^5 b_i p_i = 0$ haben die Invarianten $(\alpha)^2, (\beta)^2$ und die simultane Invariante $(\alpha\beta)$ (Nr. 1). Jene werden durch einen Büschel linearer Komplexe, diese durch einen Büschel linearer Kongruenzen verbunden; beide Büschel sind zueinander perspektiv und werden mittels eines Parameters $\varkappa$ dargestellt durch:

$$\Sigma_1^5 (a_i + \varkappa b_i) p_i = 0\,, \qquad -\infty < \varkappa < +\infty\,.$$

Die Parameterwerte $\varkappa_1$, $\varkappa_2$ der beiden speziellen Komplexe des Komplexbüschels und der beiden parabolischen Kongruenzen des Kongruenzbüschels sind die Wurzeln der Gleichung:

$$(\alpha)^2\varkappa^2 + 2(\alpha\beta)\varkappa + (\beta)^2 = 0\,.$$

Die Komplexe des Komplexbüschels und die Kongruenzen des Kongruenzbüschels haben eine und dieselbe (reelle oder imaginäre) Regelschar zweiter Ordnung gemein, bestehend aus Komplexstrahlen des linearen Komplexes Γ.

Drei lineare Kongruenzen des C_1^1-Raumes, die nicht in einem Kongruenzbüschel liegen, bestimmen einen Kongruenzbündel des C_1^1-Raumes, die mit ihnen inzidenten drei linearen Komplexe des Γ_0-Raumes bedingen in diesem einen Komplexbündel. Die linearen Kongruenzen des Kongruenzbündels und die linearen Komplexe des Komplexbündels haben zwei (reelle oder konjugiert imaginäre) Komplexstrahlen von Γ gemein. Vier unabhängige lineare Komplexe des Γ_0-Raumes werden durch ein Komplexgesbüsch verbunden, die vier mit ihnen inzidenten linearen Kongruenzen durch ein Kongruenzgebüsch.

3. Der gegebene lineare Komplex Γ bedingt sowohl in seinem C_1^1-Raume als auch in seinem Γ_0-Raume je eine polare Korrelation. Sind $\Sigma \lambda_i p_i = 0$ und $\Sigma \lambda'_i p_i = 0$ die Gleichungen zweier linearen Kongruenzen C_λ, C'_λ des C_1^1-Raumes und damit auch die Gleichungen der mit ihnen inzidenten linearen Komplexe Γ_λ, Γ'_λ des Γ_0-Raumes, so hat die bilineare Bedingung

$$\lambda_1\lambda'_1 + \lambda_2\lambda'_2 + \lambda_3\lambda'_3 + \lambda_4\lambda'_4 - \lambda_5\lambda'_5 = 0$$

einen doppelten geometrischen Ursprung:

Von den beiden linearen Kongruenzen C_λ, C'_λ geht jede im geschart involutorischen Raume der anderen in sich über. Die beiden linearen Komplexe Γ_λ, Γ'_λ sind füreinander nullinvariant, jeder von ihnen geht im Nullraume des anderen in sich über. Die beiden Leitgeraden jeder der beiden Kongruenzen sind je im geschart involutorischen Raume der anderen einander zugeordnet. Die beiden Kongruenzen haben eine (reelle oder imaginäre) Regelschar zweiter Ordnung gemein, bestehend aus Komplex-

strahlen von Γ. Die beiden Leitgeradenpaare der Kongruenzen sind daher vier Leitstrahlen dieser Regelschar. Werden die beiden linearen Kongruenzen C_λ, C'_λ als *konjugierte Kongruenzen* des C_1^1-Raumes bezeichnet, die beiden linearen Komplexe Γ_λ, Γ'_λ als *konjugierte Komplexe* des Γ_0-Raumes, so folgt:

Einer gegebenen linearen Kongruenz C_λ des C_1^1-Raumes sind die ∞^3 linearen Kongruenzen eines Kongruenzgebüsches konjugiert. Aus der Gleichung von C_λ:

Einem gegebenen linearen Komplexe Γ_λ des Γ_0-Raumes sind die ∞^3 linearen Komplexe eines Komplexgebüsches konjugiert. Aus der Gleichung von Γ_λ:

$$a_1 p_1 + a_2 p_2 + a_3 p_3 + a_4 p_4 + a_5 p_5 = 0$$

folgt die Gleichung

des Gebüsches der konjugierten Kongruenzen:

des Gebüsches der konjugierten Komplexe:

$$\lambda_1(a_5 p_1 + a_1 p_5) + \lambda_2(a_5 p_2 + a_2 p_5) + \lambda_3(a_5 p_3 + a_3 p_5) + \lambda_4(a_5 p_4 + a_4 p_5) = 0$$

oder:

$$\begin{vmatrix} \sum_1^4 \lambda_i p_i & -p_5 \\ \sum_1^4 \lambda_i a_i & a_5 \end{vmatrix} = 0.$$

Die linearen Kongruenzen und die zugehörigen Gebüsche konjugierter Kongruenzen sind als *Polkongruenzen* und *Polarkongruenzgebüsche* im polaren C_1^1-Raume des linearen Komplexes Γ einander zugeordnet, die linearen Komplexe und die zugehörigen Gebüsche konjugierter Komplexe als *Polkomplexe* und *Polarkomplexgebüsche* im polaren Γ_0-Raume von Γ.

Ist die gegebene lineare Kongruenz C_a parabolisch, der mit ihr inzidente lineare Komplex also ein spezieller Komplex (Nr. 2), so gilt:

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 - a_5^2 = 0\,.$$

In Worten:

Das Polarkongruenzgebüsch einer parabolischen Kongruenz C_a geht durch seine Polkongruenz C_a.

Das Polarkomplexgebüsch eines speziellen Komplexes Γ_a geht durch seinen Polkomplex Γ_a.

Der lineare Komplex Γ besteht aber aus den Leitgeraden der parabolischen Kongruenzen (Nr. 2) seines polaren C_1^1-Raumes und ebenso aus den Achsen der speziellen Komplexe seines Γ_0-Raumes, er ist daher das Inzidenzgebilde seines polaren C_1^1-Raumes und seines polaren Γ_0-Raumes.

4. Zwei lineare Kongruenzen des C_1^1-Raumes werden durch einen Büschel solcher Kongruenzen verbunden. Den ∞^1 Kongruenzen des Büschels sind die ∞^2 linearen Kongruenzen seines *Polarkongruenzbündels* im polaren C_1^1-Raume konjugiert. Aus der Gleichung des Kongruenzbüschels:

Zwei lineare Komplexe des Γ_0-Raumes werden durch einen Büschel solcher Komplexe verbunden. Den ∞^1 Komplexen des Büschels sind die ∞^2 linearen Komplexe seines *Polarkomplexbündels* im polaren Γ_0-Raume konjugiert. Aus der Gleichung des Komplexbüschels:

$$\sum_1^5 (a_i + \varkappa b_i)\, p_i = 0, \qquad -\infty < \varkappa < +\infty\,,$$

folgt mit Hilfe der beiden Beziehungen

$$a_1\lambda_1 + a_2\lambda_2 + a_3\lambda_3 + a_4\lambda_4 - a_5\lambda_5 = 0\,,$$
$$b_1\lambda_1 + b_2\lambda_2 + b_3\lambda_3 + b_4\lambda_4 - b_5\lambda_5 = 0$$

die Gleichung des zugeordneten

Polarkongruenzbündels: | Polarkomplexbündels:

$$\lambda_1\begin{vmatrix} p_1 & p_4 & -p_5 \\ a_1 & a_4 & a_5 \\ b_1 & b_4 & b_5 \end{vmatrix} + \lambda_2\begin{vmatrix} p_2 & p_4 & -p_5 \\ a_2 & a_4 & a_5 \\ b_2 & b_4 & b_5 \end{vmatrix} + \lambda_3\begin{vmatrix} p_3 & p_4 & -p_5 \\ a_3 & a_4 & a_5 \\ b_3 & b_4 & b_5 \end{vmatrix} = 0$$

oder:

$$\begin{vmatrix} \sum_1^3 \lambda_i p_i & p_4 & -p_5 \\ \sum_1^3 \lambda_i a_i & a_4 & a_5 \\ \sum_1^3 \lambda_i b_i & b_4 & b_5 \end{vmatrix} = 0\,.$$

Die Kongruenzen des Kongruenzbüschels und die Komplexe des Komplexbüschels gehen durch ein und dieselbe in Γ enthaltene Regelschar zweiter Ordnung. Die Strahlen dieser Regelschar sind sowohl die Leitgeraden der ∞^1 parabolischen Kongruenzen des Polarkongruenzbündels, als auch die Hauptachsen der ∞^1 speziellen Komplexe des Polarkomplexbündels.

II. Die Noethersche Abbildung.

5. Ist $\Gamma = 0$ die Gleichung eines gegebenen linearen Strahlenkomplexes Γ, so läßt sich mit ihrer Hilfe eine der Plückerschen Linienkoordinaten aus der quadratischen Plückerschen Fundamentalrelation $P^2 = 0$ (Nr. **1**) eliminieren. Die ∞^3 Strahlen des linearen Strahlenkomplexes erscheinen dann als die ∞^3 Punkte der Hyperfläche zweiter Ordnung P^2 im vierdimensionalen Raume. Ein ausgewählter Punkt A der Hyperfläche entspricht einem Komplexstrahle a. Die stereographische Projektion aus A in den diametralen dreidimensionalen Tangentialraum bildet die ∞^3 Komplexstrahlen auf die ∞^3 Punkte dieses dreidimensionalen Raumes ab. Dabei sind im dreidimensionalen Bildraume eine reelle Ebene ε und ein in ihr liegender (imaginärer oder reeller) Kegelschnitt k^2 als Fundamentalgebilde ausgezeichnet, sodaß sich die liniengeometrischen Theoreme auf einen Bildraum mit euklidischer oder pseudoeuklidischer Metrik beziehen lassen. Hat — wie in Nr. **1** — die Fundamentalrelation $P^2 = 0$ die Form

$$p_1^2 + p_2^2 + p_3^2 + p_4^2 - p_5^2 + p_6^2 = 0\,,$$

und ist $p_6 = 0$ die Gleichung des linearen Komplexes Γ, so wird nach Anfügen der stereographischen Projektion die Abbildung in rechtwinkligen Koordinaten wiedergegeben durch:

$$\varrho p_1 = 4x, \quad \varrho p_2 = 4y, \quad \varrho p_3 = 4z, \quad \varrho p_4 = x^2 + y^2 + z^2 - 4, \quad \varrho p_5 = x^2 + y^2 + z^2 + 4\,.$$

Eine gegebene lineare Kongruenz des Komplexes

$$\lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3 + \lambda_4 p_4 + \lambda_5 p_5 = 0$$

geht über in die Kugel

$$x^2 + y^2 + z^2 + \frac{4}{\lambda_4 + \lambda_5}(\lambda_1 x + \lambda_2 y + \lambda_3 z - \lambda_4 + \lambda_5) = 0\,.$$

Werden in der Kugelgleichung

$$x^2 + y^2 + z^2 - 2(\alpha x + \beta y + \gamma z) + \delta = 0$$

die Größen $\alpha, \beta, \gamma, \varrho, \delta$ als Kugelkoordinaten benutzt, wobei für den Radius ϱ die Gleichung $\alpha^2 + \beta^2 + \gamma^2 - \varrho^2 - \delta = 0$ gilt, so folgt:

$$\alpha = \frac{-2\lambda_1}{\lambda_4 + \lambda_5}, \quad \beta = \frac{-2\lambda_2}{\lambda_4 + \lambda_5}, \quad \gamma = \frac{-2\lambda_3}{\lambda_4 + \lambda_5}, \quad \varrho = \frac{2\sqrt{\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2 - \lambda_5^2}}{\lambda_4 + \lambda_5},$$

$$\delta = -\frac{4(\lambda_4 - \lambda_5)}{\lambda_4 + \lambda_5}.$$

Die parabolischen linearen Kongruenzen werden auf die Nullkugeln abgebildet. Die Orthogonalitätsbedingung zweier Kugeln $K(\alpha, \beta, \gamma, \delta, \varrho)$ und $K'(\alpha', \beta', \gamma', \delta', \varrho')$, nämlich

$$2(\alpha\alpha' + \beta\beta' + \gamma\gamma') - (\delta + \delta') = 0\,,$$

geht über in

$$\lambda_1\lambda_1' + \lambda_2\lambda_2' + \lambda_3\lambda_3' + \lambda_4\lambda_4' - \lambda_5\lambda_5' = 0\,.$$

Zwei einander senkrecht schneidende Kugeln entsprechen konjugierten linearen Kongruenzen im polaren C_1^1-Raume des Komplexes Γ. Eine Kugel und ihre Kreise gehen aus einer linearen Strahlenkongruenz und ihren Regelscharen zweiter Ordnung hervor. Die Polarentheorie des linearen Komplexes (Abschnitt I) mit ihren Begriffen Polkongruenz — Polarkongruenzgebüsch, Kongruenzbüschel — Polarkongruenzbündel usf. steht der Theorie der orthogonalen Kugeln gegenüber. Insbesondere entspricht dabei der durch eine lineare Kongruenz bedingten gescharten Involution die Inversion an einer Kugel.

6. Ein Strahlenkomplex n-ten Grades Γ_n schneidet den linearen Komplex Γ in einer Kongruenz C_n^n vom Bündel- und Feldgrade n. Sie erscheint im Punkteraum als algebraische Fläche $2n$-ter Ordnung mit dem fundamentalen Kegelschnitt k^2 als n-fache Kurve. Der Strahlenkomplex Γ_n darf dabei nicht durch den Strahl a gehen, der das Zentrum der stereographischen Projektion abgibt. Zwei Strahlenkomplexe Γ_m, Γ_n der Ordnungen m und n schneiden zwei Kongruenzen C_m^m, C_n^n in den linearen Komplex, und diese beiden Kongruenzen haben eine Regelschar $\mathfrak{R}^{2mn}$ von der Ordnung $2mn$ gemein. Die Bilder der beiden Kongruenzen C_m^m, C_n^n sind zwei Flächen von den Ordnungen $2m, 2n$. Sie enthalten den fundamentalen Kegelschnitt als m- bzw. als n-fache Kurve und durchdringen einander außerdem in einer algebraischen Raumkurve von der Ordnung $2mn$, dem Bilde der Regelschar $\mathfrak{R}^{2mn}$.

7. In der Noetherschen Abbildung repräsentieren (Fig. 1) die ∞^3 Unisekanten s des fundamentalen Kegelschnittes k^2 (die Minimalgeraden der zugehörigen Metrik) die ∞^3 Strahlenbüschel erster Ordnung des linearen Komplexes Γ. Von den ∞^3 Komplexstrahlenbüscheln liegt einer in der unendlichfernen Ebene, sein Mittelpunkt ist der unendlichferne Punkt der Komplexhauptachse. Von den ∞^3 mit dem fundamentalen Kegelschnitt inzidenten Strahlen soll nunmehr ein Strahl u als Bild dieses unendlichfernen Komplexstrahlenbüschels in der Noetherschen Abbildung ausgezeichnet werden (Fig. 1). Eine gegebene Fläche zweiter Ordnung durch den fundamentalen Kegelschnitt k^2 schneidet u in einem nicht auf k^2 liegenden Punkt S_u. Die Fläche zweiter Ordnung repräsentiert eine lineare Kongruenz und der Punkt S_u den unendlichfernen Strahl s_∞ dieser Kongruenz. Der lineare Komplex enthält ∞^2 Parallelstrahlenbüschel, je ∞^1 von ihnen gehen durch denselben unendlichfernen Komplexstrahl s und ihre Mittelpunkte erfüllen diesen Strahl. Im Bildraume entsprechen den ∞^2 Parallelstrahlenbüscheln die ∞^2 mit dem

fundamentalen Kegelschnitte und mit u inzidenten Geraden p. Je ∞^1 von ihnen gehen durch denselben Punkt S_u von u, erfüllen also einen Strahlenkegel zweiter Ordnung.

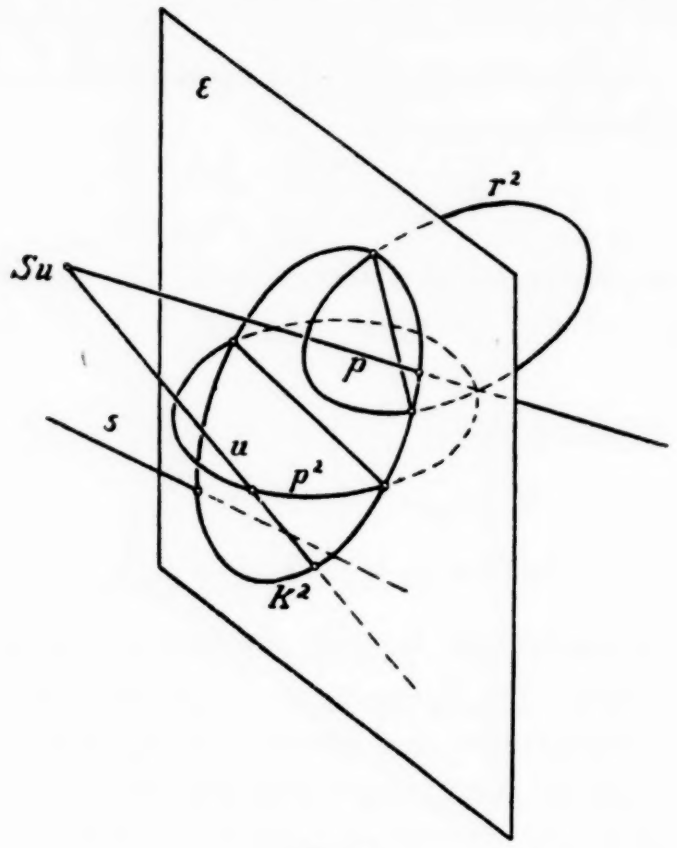

Fig. 1.

Eine Regelschar zweiter Ordnung $\mathfrak{R}^2$ des linearen Strahlenkomplexes bildet sich in einen zwei Punkte des fundamentalen Kegelschnittes enthaltenden Kegelschnitt r^2 ab. Eine parabolische Regelschar $\mathfrak{P}^2$ des Komplexes ist nunmehr dadurch ausgezeichnet, daß der entsprechende Kegelschnitt p^2 außerdem die Gerade u in einem Punkte schneidet.

III. Differentialgeometrische Eigenschaften der im linearen Strahlenkomplexe enthaltenen Regelscharen.

8. Eine gegebene Regelschar des linearen Komplexes wird durch die (erweiterte) Noethersche Abbildung in eine Raumkurve verwandelt, und es wird ein Raumkurvenpunkt P, seine Tangente t, sein Schmiegungskreis h^2 und seine Schmiegungskugel H^2 ins Auge gefaßt. Jedoch sind die Ausdrücke Schmiegungskreis und Schmiegungskugel wieder auf die Metrik des Bildraumes mit dem Kegelschnitt k^2 als Fundamentalgebilde zu beziehen. Die Schmiegungskugel des Raumkurvenpunktes P repräsentiert die lineare Schmiegungskongruenz der Regelfläche längs des Komplexstrahles p. Diese hat mit der Regelfläche vier benachbarte Strahlen gemein und schmiegt sich ihr näher an als alle übrigen linearen Kongruenzen. Im Schmiegungskreise erkennen wir die im linearen Komplexe enthaltene Regelschar des längs p oskulierenden Hyperboloides wieder.

9. Die vorhergehenden Betrachtungen ermöglichen eine besonders einfache Ableitung der wichtigsten speziellen Typen von Regelstrahlen der im linearen Komplexe enthaltenen Regelscharen.

a) *Der Torsalstrahl.*

Das Bogenelement ds einer Raumkurve im Bildraume sende seine Tangente t durch einen Punkt des fundamentalen Kegelschnittes k^2. Die Raumkurve stellt eine mit ihrer Regelschar im linearen Komplexe enthaltene Regelfläche dar, der Berührungspunkt P aber repräsentiert einen Torsalstrahl der Regelfläche. Er schneidet seinen Nachbarregelstrahl, denn er liegt mit ihm in einem Strahlenbüschel erster Ordnung, dargestellt durch die Tangente t.

b) *Der Torsalstrahl höherer Ordnung.*

Berührt im Element ds die Tangente t n-fach, so liegt ein Torsalstrahl $(n-1)$-ter Ordnung erster Art vor. Es sind n benachbarte Regelstrahlen miteinander inzident. — Konstruiert man in der Umgebung des Raumkurvenpunktes P die Tangentenfläche der Raumkurve, so mag die Tangentenfläche den fundamentalen Kegelschnitt von n-ter Ordnung berühren. Die in der Raumkurve abgebildete Regelfläche hat dann an der Stelle p einen Torsalstrahl $(n-1)$-ter Ordnung zweiter Art. Von n aufeinander folgenden Regelstrahlen schneidet jeder nur den folgenden, aber nicht den übernächsten.

c) *Der zylindrische Regelstrahl.*

Das Bogenelement der Raumkurve sende seine Tangente durch einen Punkt des fundamentalen Kegelschnittes k^2 und außerdem durch einen Punkt der Geraden u. Der durch den Berührungspunkt P dargestellte Regelstrahl liegt mit dem Nachbarregelstrahl in einem Parallelstrahlenbüschel erster Ordnung von Komplexstrahlen (7).

d) *Der Scheitelregelstrahl.*

Das oskulierende Hyperboloid der Regelfläche an der betrachteten Stelle ist durch den Kegelschnitt dargestellt, der die Bildkurve oskuliert und durch die beiden fundamentalen Punkte der Schmiegungsebene hindurchgeht (8). Bei Hyperoskulation dieses Kegelschnittes heißt der dargestellte Regelstrahl ein Scheitelregelstrahl.

e) *Der Wenderegelstrahl.*

Geht der oskulierende Kegelschnitt nicht nur durch die beiden Fundamentalpunkte der Schmiegungsebene, sondern trifft er die Gerade u noch in einem Punkte, so ist die durch den oskulierenden Kegelschnitt dargestellte oskulierende Regelfläche zweiter Ordnung ein Strahlenparaboloid (7). Der betrachtete Punkt der Raumkurve repräsentiert einen Wenderegelstrahl.

f) Der mehrfache Regelstrahl.

Ein Knotenpunkt, eine Spitze oder ein isolierter Punkt der Raumkurve im Bildraume sind bzw. die Bilder des mehrfachen Regelstrahles, des Rückkehrregelstrahles oder des isolierten Regelstrahles der Regelschar im linearen Strahlenkomplex.

Es lassen sich noch weitere spezielle Typen von Regelstrahlen auf diesem Wege charakterisieren und aus den angegebenen Typen können Singularitäten höherer Ordnung durch gegenseitige Überlagerung abgeleitet werden. Eine abwickelbare Regelschar des linearen Komplexes besteht aus Torsalstrahlen. Die Tangentenfläche ihrer Bildkurve geht daher durch den fundamentalen Kegelschnitt k^2. Den abwickelbaren Regelscharen entsprechen also die Minimalkurven des Bildraumes.

IV. Die Involutionen im linearen Strahlenkomplexe.

10. Die ∞^3 Strahlen eines linearen Strahlenkomplexes sind bekanntlich involutorisch gepaart

a) im Nullraume eines gegebenen für Γ nullinvarianten linearen Strahlenkomplexes Γ'.

b) im geschart involutorischen Raume einer gegebenen im linearen Strahlenkomplexe Γ enthaltenen linearen Strahlenkongruenz C_1^1.

c) im polaren Raume einer gegebenen einscharig im linearen Strahlenkomplexe Γ enthaltenen Regelfläche zweiten Grades R^2.

Trotz dieser dreifachen Möglichkeit sind nur zwei verschiedene Arten von Involutionen im linearen Strahlenkomplexe zu unterscheiden, denn die Fälle a) und b) führen auf dieselben Involutionen.

Die linearen Strahlenkomplexe Γ und Γ' seien füreinander nullinvariant. Dann ist im Nullraume von Γ' einem gegebenen Komplexstrahle s von Γ ein zweiter Komplexstrahl s_1 von Γ als konjugierter Strahl involutorisch zugeordnet; gehört der Strahl s_1 auch dem Komplexe Γ' an, so fällt er mit s zusammen. Die durch den Nullraum von Γ' hervorgerufene Involution im Komplexe Γ hat also ∞^2 Doppelstrahlen; sie erfüllen eine lineare Strahlenkongruenz C_1^1, die Schnittkongruenz der linearen Komplexe Γ und Γ'.

Die füreinander nullinvarianten Komplexe Γ, Γ' weisen einer gegebenen Ebene π zwei Nullpunkte P, P_1 zu, die auf einem gemeinsamen Komplexstrahle g liegen. Die Punkte P, P_1 sind homologe Punkte im geschart involutorischen Raume der linearen Kongruenz C_1^1, erfüllt von allen gemeinsamen Komplexstrahlen. Sind nähmlich wieder s, s_1 zwei im Nullraume von Γ' konjugierte Komplexstrahlen von Γ und g ein mit s und s_1 inzidenter gemeinsamer Strahl beider Komplexe, so ist der Ebene $sg = \pi$ als Nullpunkt zugeordnet

durch Γ der Punkt $s\,g = P$,
„ Γ' „ „ $s_1 g = P_1$.

Zugleich ist der Ebene $s_1 g = \pi_1$ als Nullpunkt zugeordnet

durch Γ' der Punkt $s\,g = P$.
„ Γ „ „ $s_1 g = P_1$.

Die Punkte P, P_1 und ebenso die Ebenen π, π_1 sind einander also involutorisch zugeordnet, und diese Involution ist geschart involutorisch, weil konjugierte Punkte P, P_1 auf einem gemeinsamen Strahle g der beiden Komplexe liegen und konjugierte Ebenen π, π_1 durch einen solchen Strahl gehen.

Die mit s und mit s_1 inzidenten gemeinsamen Strahlen beider linearen Komplexe liegen in der linearen Kongruenz C_1^1 und erfüllen daher eine Regelschar zweiter Ordnung. Wenn der gemeinsame Komplexstrahl g diese Regelschar durchläuft, so beschreiben die konjugierten Punkte P, P_1 des geschart involutorischen Raumes die Strahlen s, s_1. Die Komplexstrahlen s, s_1 des linearen Komplexes Γ sind also nicht nur konjugierte Strahlen im Nullraume des linearen Komplexes Γ', sondern auch konjugierte Strahlen im geschart involutorischen Raume der linearen Kongruenz C_1^1. Hiernach gilt:

Eine Involution erster Art im linearen Strahlenkomplexe ist bedingt durch den Nullraum eines für Γ nullinvarianten linearen Strahlenkomplexes Γ' und zugleich durch den geschart involutorischen Raum der den beiden Komplexen Γ und Γ' gemeinsamen linearen Kongruenz C_1^1. Konjugierte Strahlen der Involution erster Art sind sowohl im Nullraume von Γ' als auch im geschart involutorischen Raume von C_1^1 einander zugeordnet. Die Involution hat die ∞^2 Strahlen der linearen Kongruenz C_1^1 zu Doppelstrahlen.

Die zweifache Bestimmung der Involution erster Art erscheint selbstverständlich, wenn bedacht wird, daß die Polarentheorie des linearen Strahlenkomplexes Γ (Abschnitt I) zwei verschiedene Formen annimmt, je nachdem der Γ_0-Raum der ∞^4 für Γ nullinvarianten linearen Komplexe oder der C_1^1-Raum der ∞^4 in Γ enthaltenen linearen Kongruenzen den Ausgangspunkt bildet.

11. Der lineare Komplex ist polarinvariant für jede einscharig in ihm enthaltene Regelfläche R^2 zweiten Grades [3]). Hieraus folgt:

Eine Involution zweiter Art im linearen Strahlenkomplexe Γ ist bedingt durch den polaren Raum einer einscharig im linearen Komplex Γ enthaltenen Fläche zweiter Ordnung R^2.

[3]) Reye, Geometrie der Lage **2**, Stuttgart 1907, S. 117. Der Satz geht auf v. Staudt zurück.

Konjugierte Strahlen der Involution sind reziproke Polaren für die Fläche zweiter Ordnung R^2. Die Involution hat die ∞^1 Regelstrahlen von R^2 zu Doppelstrahlen.

Der lineare Strahlenkomplex trägt ∞^4 Involutionen erster Art und ∞^6 Involutionen zweiter Art. Von einer Klassifikation dieser Involutionen im einzelnen soll hier abgesehen werden.

12. Will man sich in der Geometrie des linearen Strahlenkomplexes Γ mit dem Effekt der Noetherschen Abbildung begnügen, so scheinen die Überlegungen der Nr. **10** und **11** entbehrlich zu sein. Die Kollineationen des linearen Komplexes in sich werden nach Anwendung der Noetherschen Abbildung durch quadratische Cremonatransformationen im dreidimensionalen Bildraume wiedergegeben. Es gibt zwei Arten involutorischer quadratischer Cremonatransformationen, und aus ihnen ist auf die beiden Arten von Involutionen im linearen Strahlenkomplex zu schließen.

Die eine involutorische quadratische Transformation ist durch die Inversion dargestellt. Eine Fläche zweiter Ordnung C^2 durch den fundamentalen Kegelschnitt k^2 ordnet der Ebene ε dieses Kegelschnittes den Pol C zu; zwei inverse Punkte P, P_1 liegen auf demselben Strahle durch das Inversionszentrum C, jeder in der Polarebene des andern. — Das Zentrum C werde als Ecke $x_1 = x_2 = x_3 = 0$ des Koordinatentetraeders gewählt, die Ebene ε als $x_4 = 0$. Es sei $\varphi^2(x_1, x_2, x_3) = 0$ die Gleichung des Kegels aus C durch den fundamentalen Kegelschnitt k^2, sodaß sich die Gleichung der Fläche C^2 schreibt:

$$\varphi^2(x_1, x_2, x_3) - cx_4^2 = 0 \qquad (c \text{ Konstante}).$$

Dann ist die Inversion wiedergegeben durch:

$$x_1' : x_2' : x_3' : x_4' = x_1 x_4 : x_2 x_4 : x_3 x_4 : \frac{\varphi^2(x_1, x_2, x_3)}{c}.$$

Damit ist die Involution erster Art im linearen Komplex Γ durch eine Inversion dargestellt. Es ist auch ersichtlich, daß die Involution durch den geschart involutorischen Raum einer im Komplexe enthaltenen linearen Kongruenz C_1^1 hervorgerufen wird, weil die Inversion die ∞^2 Punkte der Fläche zweiter Ordnung C^2 zu Fixpunkten hat. Daß dieselbe Involution auch durch den Nullraum eines für den linearen Komplex Γ nullinvarianten linearen Strahlenkomplexes Γ' bedingt wird (**10**), geht aus der Noetherschen Abbildung allein nicht hervor, weil der dreidimensionale Bildraum die Geometrie des linearen Komplexes von innen, aber nicht von außen zeigt. Dasselbe Mißgeschick erleidet die Polarentheorie des Komplexes bei der Abbildung. Die Vorteile der Abbildung liegen hier in anderer Richtung:

13. Die Wahl des unendlichfernen Kugelkreises zum fundamentalen Kegelschnitte k^2 führt die Darstellung der Involution erster Art auf die Transformation durch reziproke Radienvektoren an einer (reellen oder imaginären) Kugel zurück. Die Kugel C^2 und ihre ∞^3 Orthogonalkugeln repräsentieren eine lineare Kongruenz C_1^1 und das zugehörige Polargebüsch der ∞^3 konjugierten linearen Kongruenzen; jede von ihnen ist im geschart involutorischen Raum von C_1^1 invariant.

Die durch eine Inversion an einer Kugel in sich überführbaren Flächen hat Moutard[4]) behandelt und als *anallagmatische* Flächen bezeichnet. Sie werden hier *selbstinverse* Flächen genannt. Eine für die Kugel C^2 selbstinverse Fläche F ist Hüllfläche von ∞^2 Orthogonalkugeln von C^2. Die ∞^2 Mittelpunkte der umhüllten Kugeln erfüllen eine Fläche, den

[4]) Moutard, Sur la transformation par rayons vecteurs réciproques, Nouv. Ann. (2) **3** (1864), S. 306—309. — Sur les surfaces anallagmatiques du quatrième ordre, ebenda S. 536—539.

Deferenten D. (In besonderen Fällen umhüllt F nur ∞^1 Orthogonalkugeln, deren Mittelpunkte eine Kurve erfüllen.) Die selbstinverse Fläche F ist durch ihren Deferenten bestimmt. Um einen herausgegriffenen Punkt O des Deferenten schlagen wir die Orthogonalkugel O^2 zur Inversionskugel C^2 und legen in O an den Deferenten D die Tangentialebene γ. Das Lot vom Inversionszentrum auf die Tangentialebene γ schneidet die Orthogonalkugel in ihren beiden (zueinander inversen) Berührungspunkten G, G_1 mit der selbstinversen Hüllfläche F.

Die selbstinverse Fläche F repräsentiert eine im linearen Komplex enthaltene Strahlenkongruenz C_f. Die ∞^2 Strahlen dieser Kongruenz C_f sind im geschart involutorischen Raum der linearen Kongruenz C_1^1 involutorisch gepaart. Wird eine solche Kongruenz als *involutorisch selbstgescharte* Kongruenz bezeichnet, so gilt:

Eine für die lineare Kongruenz C_1^1 involutorisch selbstgescharte Kongruenz C_f geht im geschart involutorischen Raume von C_1^1 in sich über. In je zwei konjugierten Kongruenzstrahlen wird die Kongruenz von einer involutorisch selbstgescharten linearen Kongruenz berührt. Eine involutorisch selbstgescharte Kongruenz C_f umhüllt also ∞^2 involutorisch selbstgescharte lineare Kongruenzen und jede Hüllkongruenz involutorisch selbstgescharter linearer Kongruenzen ist involutorisch selbstgeschart.

Zu bemerken ist, daß zwei selbstinverse Flächen des Bildraumes einander in einer selbstinversen Raumkurve durchdringen und daß diese Raumkurven die involutorisch selbstgescharten Regelscharen des linearen Strahlenkomplexes darstellen.

Die hier dargelegten Theoreme über die Geometrie des linearen Strahlenkomplexes führen uns auf manche neuen Fragestellungen und sollen in einer weiteren Arbeit behandelt werden.

Eingegangen 9. September 1935

Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f.

Von *Ernst Witt* in Göttingen.

Es ist eine bekannte Frage aus der Körpertheorie, ob es bei festem Grundkörper R und zu vorgegebener endlicher Gruppe $\mathfrak{G}$ galoissche Körper K/R mit einer zu $\mathfrak{G}$ isomorphen Gruppe gibt. Es ist eine weitere Aufgabe, alle derartigen Körper wirklich zu konstruieren.

In dieser Arbeit soll die vollständige Lösung gegeben werden für den Fall, daß der Grundkörper R die Charakteristik p hat, und daß $\mathfrak{G}$ eine p-Gruppe ist.

a durchlaufe alle Zahlen des Grundkörpers. In dieser additiven Gruppe bilden die Zahlen $a^p - a$ eine Untergruppe vom Index

$$(a : a^p - a) = p^N \qquad (N = 0, 1, \ldots \infty).$$

n sei die kleinstmögliche Anzahl von Erzeugenden der Gruppe $\mathfrak{G}$. Ferner sei p^f die Ordnung von $\mathfrak{G}$, und Ω die Anzahl aller Automorphismen der Gruppe $\mathfrak{G}$.

Wir werden folgendes Resultat beweisen:

Satz. *Für die Existenz von galoisschen Körpern K/R zur Gruppe $\mathfrak{G}$ ist die Bedingung*

$$n \leqq N$$

notwendig und auch hinreichend. Für $N = \infty$ gibt es zu jeder p-Gruppe unendlich viele Körper. Falls N eine endliche Zahl ist, ist die Anzahl der verschiedenen Körper zur Gruppe $\mathfrak{G}$ genau

$$\frac{1}{\Omega}\, p^{N(f-n)}(p^N - 1)\,(p^N - p) \cdots (p^N - p^{n-1}) \qquad (n \leqq N).$$

Das erste Ergebnis in dieser Richtung erzielten Artin und Schreier[1]). Sie zeigten, daß R immer einen zyklischen Oberkörper vom Grade p^2 besitzt, wenn ein solcher vom Grad p vorhanden ist ($N \geqq 1$). Neuerdings hat Albert[2]) unter derselben Voraussetzung auch die Existenz eines zyklischen Oberkörpers vom Grade p^f nachgewiesen. Die Art der Körperkonstruktion hängt eng zusammen mit einem Satz von R. Brauer[3]) über verschränkte Produkte. —

Am Schluß werden wir für eine *beliebige Körpercharakteristik* alle Körper mit *Quaternionengruppe* konstruieren.

---

[1]) E. Artin und O. Schreier, Über eine Kennzeichnung der reell abgeschlossenen Körper, Abh. Math. Sem. Hamburg **5** (1927).

[2]) A. A. Albert, Cyclic fields of degree p^n over F of characteristic p, Bull. Am. Math. Soc. **40** (1934).

[3]) R. Brauer, Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind, Crelle **168** (1932), Satz 7. — Vgl. vor allem die Schlußbemerkung von H. Hasse zu seiner Lösung der Aufgabe 156, Jahresber. der D. M. V. **44** (1934), *63/64*.

I. *Bemerkungen über p-Gruppen.*

In der Gruppe $\mathfrak{G}$ bilden wir die Untergruppe $\mathfrak{G}^*$, die von allen Elementen der Form $xyx^{-1}y^{p-1}$ erzeugt wird. Diese charakteristische Untergruppe $\mathfrak{G}^*$ enthält $y^p = 1y1^{-1}y^{p-1}$ und $xyx^{-1}y^{-1} = xyx^{-1}y^{p-1}\cdot y^{-p}$; umgekehrt wird $\mathfrak{G}^*$ von allen Kommutatoren und p-ten Potenzen erzeugt wegen $xyx^{-1}y^{p-1} = xyx^{-1}y^{-1}\cdot y^p$. $\mathfrak{G}/\mathfrak{G}^*$ ist die größte abelsche Faktorgruppe vom Exponenten p.

$\mathfrak{G}$ habe die Ordnung p^l, es sei $(\mathfrak{G}:\mathfrak{G}^*) = p^n$. Burnside *hat bewiesen, daß sich* $\mathfrak{G}$ *durch* n*, aber nicht durch weniger Gruppenelemente erzeugen läßt.* Ferner ist die Anzahl Ω der Automorphismen von $\mathfrak{G}$ ein Teiler der Zahl

$$\bar{\Omega} = p^{n(l-n)}(p^n - 1)\,(p^n - p)\cdots(p^n - p^{n-1})\,.$$

Für diese Tatsache hat Hall [4]) einen einfachen Beweis gegeben.

Ein Normalteiler $\mathfrak{N} \neq 1$ von $\mathfrak{G}$ enthält stets Elemente $\neq 1$, die im Zentrum $\mathfrak{Z}$ von $\mathfrak{G}$ liegen. Das folgt in bekannter Weise aus der Zerlegung von $\mathfrak{N}$ in Klassen bezüglich $\mathfrak{G}$ konjugierter Elemente.

Es sei $\mathfrak{G}^* \neq 1$. Dann gibt es eine Untergruppe $\mathfrak{g} \neq 1$ vom Exponenten p, die in $\mathfrak{Z} \cap \mathfrak{G}^*$ liegt. Wenn $\mathfrak{g}$ möglichst groß gewählt wird, ist $\mathfrak{g}$ eine charakteristische Untergruppe von $\mathfrak{G}$.

Die Elemente der Untergruppe $\mathfrak{g}$ seien mit $g, g_1, \ldots$ bezeichnet, die Elemente der Faktorgruppe $\Gamma = \mathfrak{G}/\mathfrak{g}$ mit $\varrho, \sigma, \tau, \ldots$; u_σ sei ein Vertreter der Nebengruppe σ.

$\mathfrak{G}$ läßt sich als verschränktes Produkt darstellen durch die Formeln:

$$u_\sigma u_\tau = g_{\sigma,\tau} u_{\sigma\tau} \tag{1a}$$

$$u_\sigma g = g\, u_\sigma \tag{1b}$$

$$g_{\sigma,\tau} g_{\varrho,\sigma\tau} = g_{\varrho,\sigma} g_{\varrho\sigma,\tau}\,. \tag{1c}$$

Hilfssatz. *Es gibt genau* $(\mathfrak{g}:1)^n$ *Automorphismen der Gruppe* $\mathfrak{G}$*, die alle Nebengruppen von* $\mathfrak{g}$ *festlassen.*

Beweis. Ein solcher Automorphismus A läßt alle Elemente von $\mathfrak{G}^*$ fest, denn aus $x_i^A = g_i x_i$ folgt $(x_1 x_2 x_1^{-1} x_2^{p-1})^A = x_1 x_2 x_1^{-1} x_2^{p-1}$. Erst recht bleiben die Elemente von $\mathfrak{g}$ fest. Es sei $u_\sigma^A = g_\sigma u_\sigma$. Wird A auf die Gleichung (1a) angewandt, so folgt $g_\sigma g_\tau = g_{\sigma\tau}$. Umgekehrt wird durch jede homomorphe Abbildung $\sigma \to g_\sigma$ ein Automorphismus A der Gruppe $\mathfrak{G}$ festgelegt, der jede Nebengruppe von $\mathfrak{g}$ festläßt. Da $\mathfrak{g}$ abelsch vom Exponenten p ist, gehen bei jeder solchen Abbildung die Elemente von Γ^* in 1 über. Es ist $\Gamma^* = \mathfrak{G}^*/\mathfrak{g}$, also $(\Gamma:\Gamma^*) = p^n$. Nun gibt es genau $(\mathfrak{g}:1)^n$ Abbildungen von Γ/Γ^* auf $\mathfrak{g}$ und damit auch von Γ auf $\mathfrak{g}$, w. z. b. w.

II. *Analyse.*

Um einen passenden Ansatz für die Konstruktion aller Körper mit der Gruppe $\mathfrak{G}$ zu finden, beginnen wir mit der Analyse.

In einer früheren Arbeit [5]) findet sich im Abschnitt III die vollständige Behandlung der *abelschen Körper vom Exponenten* p. Deshalb *genügt es hier,* $\Gamma^* \neq 1$ *vorauszusetzen.* Dieser Arbeit entnehmen wir auch die Bezeichnung $\wp x = x^p - x$, ferner werden wir im nächsten Abschnitt von den Sätzen W. I, 2 und W. I, 3 über Summandensysteme wesentlich Gebrauch machen.

---

[4]) P. Hall, A contribution to the theory of groups of prime-power order, Proc. Lond. Math. Soc. (2) **36** (1934), 35/36.

[5]) E. Witt, Der Existenzsatz für abelsche Funktionenkörper, dieses Journal **173** (1935). — Die Resultate dieser Arbeit werden hier mit W. I, 3 usw. zitiert.

Es liege ein galoischer Körper K/R vor, dessen Automorphismengruppe die vorhin beschriebene Gruppe $\mathfrak{G}$ ist. Der Untergruppe $\mathfrak{g}$ entspreche der galoissche Zwischenkörper k.

Da K/k abelsch vom Exponenten p ist, kann $K = k(\theta^1, \ldots, \theta^r)$ gesetzt werden, wobei $p^r = (\mathfrak{g} : 1)$ ist, und jedes θ^ν einer Gleichung

$$\wp\theta^\nu = \gamma^\nu \tag{2}$$

genügt ($\nu = 1, \ldots, r$ ist ein Index). Wenden wir auf (2) die Operation $g - 1$ an, so sehen wir, daß

$$(g-1)\,\theta^\nu = \chi^\nu(g) \tag{3}$$

im Primkörper liegt. Die Funktion χ^ν ist ein additiver Charakter der Gruppe $\mathfrak{g}$, und zwar bilden diese χ^ν eine Basis für alle Charaktere χ von $\mathfrak{g}$ (W. III). Aus (2) folgt

$$(g-1)\,(u_\sigma - 1)\,\theta^\nu = (u_\sigma - 1)\,(g-1)\,\theta^\nu = (u_\sigma - 1)\,\chi^\nu(g) = 0\,,$$

daher liegt

$$(u_\sigma - 1)\,\theta^\nu = \delta^\nu_\sigma \tag{4}$$

in k. Auf diese Gleichung werde die Operation $\wp$ angewandt, wir erhalten dann

$$(\sigma - 1)\gamma^\nu = \wp\delta^\nu_\sigma\,. \tag{5}$$

Endlich berechnen wir

$$\begin{aligned}\delta^\nu_\sigma + \sigma\delta^\nu_\tau - \delta^\nu_{\sigma\tau} &= [(u_\sigma - 1) + u_\sigma(u_\tau - 1) - (u_{\sigma\tau} - 1)]\,\theta^\nu \\ &= u_{\sigma\tau}(g_{\sigma,\tau} - 1)\,\theta^\nu = u_{\sigma\tau}\chi^\nu(g_{\sigma,\tau}) = \chi^\nu(g_{\sigma,\tau})\,,\end{aligned}$$

also

$$\delta^\nu_\sigma + \sigma\delta^\nu_\tau - \delta^\nu_{\sigma\tau} = \chi^\nu(g_{\sigma,\tau})\,. \tag{6}$$

III. *Konstruktion.*

Indem wir gewissermaßen die Betrachtungen des vorigen Abschnitts umkehren, gelangen wir tatsächlich zu einer Konstruktionsmethode, die uns alle Körper K/R mit der vorgeschriebenen Gruppe $\mathfrak{G}$ liefert. Es sei wieder $\mathfrak{G}^* \neq 1$.

$\chi(g)$ sei eine homomorphe Abbildung der Gruppe $\mathfrak{g}$ auf die additive Gruppe der Primkörperzahlen. Es gibt $(\mathfrak{g} : 1) = p^r$ verschiedene derartige Charaktere χ der Gruppe $\mathfrak{g}$. Mit $\chi^1, \ldots, \chi^r$ bezeichnen wir eine Basis für alle Charaktere χ. Aus (1c) folgt

$$\chi^\nu(g_{\sigma,\tau}) + \chi^\nu(g_{\varrho,\sigma\tau}) = \chi^\nu(g_{\varrho,\sigma}) + \chi^\nu(g_{\varrho\sigma,\tau})\,. \tag{7}$$

Die Körperkonstruktion führen wir schrittweise aus. Wir nehmen an, wir hätten schon einen Körper k/R, dessen galoissche Gruppe mit der gegebenen Gruppe Γ isomorph ist. Wir denken uns eine bestimmte Isomorphie zu Grunde gelegt: Dem Gruppenelement σ entspreche der Körperautomorphismus s.

Infolge der Gleichung (7) können wir den Satz W. I, 3 über Summandensysteme anwenden:

$$\chi^\nu(g_{\sigma,\tau}) = \delta^\nu_s + s\delta^\nu_t - \delta^\nu_{st} \tag{8}$$

ist mit Zahlen δ^ν_s aus dem Körper k lösbar. Es folgt

$$\wp\delta^\nu_s + s\wp\delta^\nu_t - \wp\delta^\nu_{st} = 0\,,$$

und nach W. I, 2 ist deshalb

$$\wp\delta^\nu_s = (s-1)\gamma^\nu \tag{9}$$

mit Zahlen γ^ν aus dem Körper k lösbar.

Ohne die Richtigkeit der Formeln (7), (8), (9) zu verletzen, dürfen wir jedenfalls [(a) kommt später]

(b) χ^ν, δ_s^ν, γ^ν simultan einer linearen Transformation unterwerfen, deren Koeffizienten ganze Zahlen mod p sind,

(c) simultan δ_s^ν durch $\delta_s^\nu + (s-1)\alpha^\nu$, γ^ν durch $\gamma^\nu + \wp\alpha^\nu$ ersetzen (α^ν aus k).

Nun wollen wir die Möglichkeit einer Gleichung $\Sigma x_\nu \gamma^\nu = \wp\beta$ widerlegen, in der nicht alle Zahlen $x_\nu \equiv 0 \bmod p$ sind. Wegen (b) genügt es, $\gamma^1 = \wp\beta$ zu widerlegen, und wegen (c) brauchen wir nur zu zeigen, daß $\gamma^1 = 0$ unmöglich ist.

Es sei $\gamma^1 = 0$, dann liegt wegen (9) δ_s^1 im Primkörper, und wir können $\delta_s^1 = \chi^1(g_\sigma)$ setzen. Die Gleichung (8) lautet jetzt

$$\chi^1(g_{\sigma,\tau}) = \chi^1(g_\sigma) + \chi^1(g_\tau) - \chi^1(g_{\sigma\tau}). \tag{9'}$$

$\mathfrak{g}_1$ sei die Untergruppe von $\mathfrak{g}$, die durch $\chi^1(g) = 0$ bestimmt wird. Wir betrachten die Gruppe $\mathfrak{G}$ jetzt nur noch mod $\mathfrak{g}_1$. Die Beziehung $\mathfrak{G}^* \geqq \mathfrak{g} > 1$ bleibt dann bestehen. Andererseits folgt aus (9'), daß die Elemente $g_\sigma^{-1} u_\sigma$ untereinander eine Gruppe $\mathfrak{U}$ bilden, und zwar wird $\mathfrak{G} = \mathfrak{g} \times \mathfrak{U}$, folglich $\mathfrak{G}^* = \mathfrak{U}^*$. $\mathfrak{G}^*$ ist also doch fremd zu $\mathfrak{g}$, und das ist ein Widerspruch.

Wir haben also gezeigt, daß die Zahlen γ^ν linear unabhängig sind bezüglich der Zahlen $\wp\beta$. θ^ν sei eine Wurzel der Gleichung

$$\wp x = \gamma^\nu . \tag{10}$$

Wir bilden nun den Körper $K = k(\theta_1, \ldots, \theta_r)$. Nach W. III ist $(K : k) = p^r$, also $(K : R) = p^l$. Durch

$$\bar{g}\theta^\nu = \theta^\nu + \chi^\nu(g), \qquad \bar{g}\alpha = \alpha \tag{11}$$

wird ein Automorphismus $\bar{g}$ von K/k erklärt. Da $\theta^\nu + \delta_s^\nu$ wegen (9) der Gleichung $\wp x = s\gamma^\nu$ genügt, wird durch

$$v_s\theta^\nu = \theta^\nu + \delta_s^\nu, \qquad v_s\alpha = s\alpha \tag{12}$$

ein Automorphismus v_s von K/R festgelegt. Jetzt behaupten wir

$$v_s v_t = \overline{g_{\sigma,\tau}} v_{st}, \tag{13a}$$

$$v_s \bar{g} = \bar{g} v_s . \tag{13b}$$

Für die Zahlen von k stimmen diese Regeln natürlich, daher müssen wir nur noch ihre Gültigkeit bei Anwendung auf die Zahlen θ^ν prüfen: Es ist

$$v_s v_t \theta^\nu = v_s(\theta^\nu + \delta_t^\nu) = \theta^\nu + \delta_s^\nu + s\delta_t^\nu ,$$

$$\overline{g_{\sigma,\tau}} v_{st}\theta^\nu = \overline{g_{\sigma,\tau}}(\theta^\nu + \delta_{st}^\nu) = \theta^\nu + \chi^\nu(g_{\sigma,\tau}) + \delta_{st}^\nu ,$$

und wegen (8) stimmen beide Zeilen überein; entsprechend wird (13b) bewiesen.

Damit haben wir offensichtlich gezeigt, daß K/R galoisch mit einer zu $\mathfrak{G}$ isomorphen Gruppe ist.

Ergebnis. *k/R sei galoisch mit einer zu Γ isomorphen Gruppe. Dann erhalten wir auf folgende Weise jeden Oberkörper K/R mit einer zu $\mathfrak{G}$ isomorphen Gruppe: Wir wählen beliebig*

(A) *eine isomorphe Abbildung von Γ auf die Automorphismengruppe von k/R: $\sigma \to s$,*

(B) *eine Basis χ^ν für die additiven Charaktere χ von $\mathfrak{g}$,*

(C) *eine Lösung δ_s^ν von $\chi^\nu(g_{\sigma,\tau}) = \delta_s^\nu + s\delta_t^\nu - \delta_{st}^\nu$ (W. I, 3),*

(D) *eine Lösung γ^ν von $\wp\delta_s^\nu = (s-1)\gamma^\nu$ (W. I, 2)*

und adjungieren sämtliche Wurzeln der Gleichungen $\wp x = \gamma^\nu$ zu k. Die Abbildung von $\mathfrak{G}$ auf die galoissche Gruppe von K/R läßt sich ferner so einrichten, daß sie die schon gewählte Abbildung (A) *fortsetzt.*

Bemerkung. Für eine Grundkörper R, dessen Charakteristik $\neq p$ ist, der aber die p-ten Einheitswurzeln enthält, lassen sich beinahe alle Überlegungen zur Konstruktion von Körpern K/R zu einer gegebenen p-Gruppe im multiplikativer Fassung durchführen. (Für die Elemente des Primkörpers sind die Einheitswurzeln zu nehmen, statt $\wp x$ ist x^p zu setzen, W. I, 2 läßt sich durch W. I, 1 ersetzen.) Nur das analoge Gleichungssystem

$$(c') \qquad \chi^\nu(g_{\sigma,\tau}) = \frac{\delta_s^\nu (\delta_t^\nu)^s}{\delta_{st}^\nu}$$

braucht nicht immer lösbar zu sein, sondern das Zerfallen der Algebren $(\chi^\nu(g_{\sigma,\tau}), k)$ wird hier zum Kriterium für die Existenz eines Körpers K. Auch wenn es über dem Grundkörper R keine Algebren vom Exponenten p gibt, ist (c′) im Gegensatz zu (c) im allgemeinen nur theoretisch lösbar, aber sonst bleibt dann die ganze Theorie richtig.

IV. *Abzählung.*

Statt der Abbildung $\sigma \to s$ in (A) werde eine andere Abbildung $\bar{\sigma} \to s$ zugrunde gelegt. Unter welchen Umständen ist es möglich, daß durch passende Wahl in (B), (C), (D) trotzdem derselbe Körper K erscheint? Die letzten Zeilen im oben formulierten Ergebnis führen zur Antwort:

(a) Genau dann, wenn der Automorphismus $\sigma \to \bar{\sigma}$ von Γ durch einen Automorphismus von $\mathfrak{G}$ induziert wird.

In (B) werde eine andere Basis für die Charaktere zugrunde gelegt. Aus (b) folgt, daß stets durch eine passende Wahl der Lösungen in (C) und (D) derselbe Körper K erreichbar ist.

In (C) werde eine andere Lösung gewählt. Nach W. I, 2 hat die Differenz beider Lösungen die Form $(\sigma - 1)\alpha^\nu$. Aus (c) folgt, daß durch eine passende Änderung in (D) derselbe Körper K entsteht.

Jede neue Lösung von (D) hat die Form $\gamma^\nu + b^\nu$, wobei b^ν in R liegt. Wann führt sie zum selben Körper K? Die Antwort lautet:

(d) Genau dann, wenn $b^\nu = \wp\beta^\nu$ ist, wobei β^ν in k liegt. (Nach W. III erzeugen die zulässigen β^ν gerade den zur Untergruppe Γ^* gehörigen größten abelschen Unterkörper k^* vom Exponenten p.)

N sei endlich. Wir können nun feststellen, wieviel Körper K es über k gibt. Dazu genügt es, noch anzunehmen, daß $\mathfrak{g}$ eine charakteristische Untergruppe von $\mathfrak{G}$ ist. ω sei die Anzahl der Automorphismen der Gruppe Γ, ω_1 sei die Anzahl derjenigen Automorphismen von Γ, die von Automorphismen von $\mathfrak{G}$ induziert werden. Nach dem in I bewiesenen Hilfssatz ist $\omega_1 = \Omega/p^{rn}$. In (A) gibt es ω/ω_1 wesentlich verschiedene Möglichkeiten der Wahl, in (D) gibt es $p^{r(N-n)}$ wesentlich verschiedene Möglichkeiten. Also gibt es genau

$$\frac{\omega}{\omega_1} p^{r(N-n)} = \frac{\omega}{\Omega} p^{rN}$$

verschiedene Körper K über demselben Körper k.

Jedem Körper K ist eindeutig ein Unterkörper k zugeordnet, d. h. unabhängig davon, wie die Automorphismen von K/R bezeichnet werden. Da es nach Induktionsannahme im ganzen

$$\frac{1}{\omega} p^{N(f-r-n)}(p^N - 1)(p^N - p) \cdots (p^N - p^{n-1})$$

verschiedene Körper k mit der Gruppe Γ gibt, ist die Anzahl der verschiedenen Körper K mit der Gruppe $\mathfrak{G}$ genau

$$\frac{1}{\Omega}\, p^{N(f-n)}(p^N-1)\,(p^N-p)\cdots(p^N-p^{n-1}), \qquad \text{q. e. d.}$$

Bemerkung. $\mathfrak{G}$ sei eine p-Gruppe mit möglichst vielen Automorphismen, d. h. es sei $\Omega = \bar{\Omega}$. Dies ist z. B. der Fall für eine zyklische Gruppe, allgemein für eine abelsche Gruppe vom Typus $(p^s, p^s, \ldots, p^s)$ oder für die Quaternionengruppe oder für eine Gruppe der Ordnung p^3, in der jedes Element die Ordnung p hat. Dann erreicht die Zahl ω_1 die für die Faktorgruppe Γ gültige obere Schranke, also ist $\omega_1 = \omega = \bar{\omega}$. (Alle echten charakteristischen Untergruppen von $\mathfrak{G}$ liegen in $\mathfrak{G}^*$. Durch Induktion kann leicht gezeigt werden, daß alle Automorphismen einer charakteristischen Faktorgruppe durch Automorphismen von $\mathfrak{G}$ induziert werden, und daß die Faktorgruppe wieder möglichst viele Automorphismen besitzt.)

Bei der Konstruktion von Körpern K zu einer Gruppe $\mathfrak{G}$ mit möglichst vielen Automorphismen kommt es also nicht wesentlich darauf an, welche Abbildung in (A) zugrunde gelegt wird. Da es sowieso auch nicht auf die Wahl in (B) und (C) ankommt, genügt es, die Lösungen von (D) zu variieren, um zu allen Körpern K zu gelangen.

V. *Konstruktion zyklischer Körper.*

Wenn es sich um eine zyklische Gruppe $\mathfrak{G}$ der Ordnung p^f handelt, lassen sich die bisherigen Überlegungen etwas einfacher gestalten. Das möge hier kurz geschehen.

k/R sei ein zyklischer Körper vom Grade p^{f-1} $(f>1)$, die Charakteristik sei p. Mit s bezeichnen wir irgendeinen erzeugenden Automorphismus von k/R, mit Sp die Spurbildung. χ sei eine Zahl $\neq 0$ aus dem Primkörper.

Analyse. $K = k(\theta)$ sei ein gegebener Körper, der über R zyklisch vom Grade p^f ist. S sei ein Automorphismus von K/R, der die Fortsetzung von s ist. S erzeugt die Gruppe von K/R, und $S^{p^{f-1}} = g$ die Gruppe von K/k. Es darf angenommen werden, daß θ einer Artin-Schreierschen Gleichung $\wp\theta = \gamma$ genügt, und daß $(g-1)\theta = \chi$ gilt. Wegen $(g-1)(S-1)\theta = (S-1)(g-1)\theta = (S-1)\chi = 0$ liegt $(S-1)\theta = \delta$ schon im Körper k. Es folgt jetzt $(s-1)\gamma = \wp\delta$ und

$$\mathrm{Sp}\,\delta = \frac{S^{p^{f-1}}-1}{S-1}(S-1)\theta = (g-1)\theta = \chi.$$

Konstruktion. Nach W. I gibt es eine Zahl δ mit $\mathrm{Sp}\,\delta = \chi$. Ferner hat wegen $\mathrm{Sp}\,\wp\delta = 0$ auch die Gleichung $(s-1)\gamma = \wp\delta$ eine Lösung γ.

Ohne Änderung der Formeln darf gleichzeitig δ durch $\delta + (s-1)\alpha$ und γ durch $\gamma + \wp\alpha$ ersetzt werden.

Um $\gamma \neq \wp\beta$ zu beweisen, genügt es daher, $\gamma = 0$ zu widerlegen. Aus $\gamma = 0$ würde $\wp\delta = 0$, also $\mathrm{Sp}\,\delta = 0$ folgen, und das ist ein Verstoß gegen $\mathrm{Sp}\,\delta = \chi$.

θ sei eine Wurzel der Gleichung $\wp x = \gamma$. $K = k(\theta)$ hat über R den Grad p^f. Weil $\theta + \delta$ der Gleichung $\wp x = s\gamma$ genügt, wird durch

$$S\theta = \theta + \delta, \qquad S\alpha = s\alpha$$

ein Automorphismus von K/R festgelegt. Wegen $S^{p^{f-1}}\theta = \theta + \mathrm{Sp}\,\delta \neq \theta$ hat S die Ordnung p^f. Daher ist K/R zyklisch, und S ist ein erzeugender Automorphismus. Es ist noch $K = R(\theta)$ zu bemerken.

Ergebnis. *k/R sei zyklisch vom Grad p^{f-1} $(f>1)$. Dann erhalten wir auf folgende Weise jeden zyklischen Oberkörper K/R vom Grad p^f: Wir wählen beliebig*

(A) *einen erzeugenden Automorphismus* s *von* $k|R$,
(B) *eine Zahl* $\chi \neq 0$ *aus dem Primkörper*,
(C) *eine Lösung* δ *von* $\mathrm{Sp}\,\delta = \chi$,
(D) *eine Lösung* γ *von* $(s-1)\gamma = \wp\delta$
und adjungieren eine Wurzel θ *der Gleichung* $\wp x = \gamma$ *zu* R. *Alle anderen Körper dieser Art gewinnen wir dadurch, daß wir* γ *durch* $\gamma + r$ *ersetzen* (r *aus* R).

Versehen wir die Zahlen χ, δ, γ, θ mit einem Index f, um den Schritt $(f-1)/f$ anzudeuten, so können wir etwa $\chi_f = (-1)^{f-1}$ und $\delta_f = (\theta_1 \cdots \theta_{f-1})^{p-1}$ wählen — dadurch erhalten wir genau die Formeln von Albert [2]) wieder.

Bemerkung. Wenn die Charakteristik $\neq p$ ist, aber k eine p-te Einheitswurzel $\chi \neq 1$ enthält, so lautet das zu lösende Gleichungssystem:

$$\text{(14)} \qquad \mathrm{Norm}\,\delta = \chi, \qquad \gamma^{s-1} = \delta^p .$$

Die erste Gleichung ist genau dann lösbar, wenn die zyklische Algebra (χ, k, s) zerfällt; dagegen hat die zweite immer eine Lösung.

Beispiel. Konstruktion der zyklischen Körper vierten Grades, die einen festen Körper $R(\sqrt{a})$ enthalten (Charakteristik $\neq 2$).

Damit es solche Körper K überhaupt gibt, muß $\chi = -1$ Norm einer Zahl aus $R(\sqrt{a})$ sein, d. h. $a = b^2 + c^2$ muß in R lösbar sein. Ist umgekehrt $a = b^2 + c^2$, so ist sicher $c \neq 0$, und durch

$$\delta = \frac{b - \sqrt{a}}{c}, \qquad \gamma = a + b\sqrt{a}$$

werden in der Tat beide Gleichungen (14) gelöst. Folglich werden dann durch

$$K = R(\sqrt{r\,(a + b\sqrt{a})})$$

alle derartigen Körper gegeben, indem r alle Zahlen $\neq 0$ aus R durchläuft.

VI. *Konstruktion von Quaternionenkörpern.*

Erster Fall. Der Grundkörper habe die Charakteristik 2. k sei ein Körper mit der Vierergruppe $\Gamma = (e, \sigma_1, \sigma_2, \sigma_3)$, $R(\xi_\nu)$ sei der zur Untergruppe (e, σ_ν) gehörige quadratische Unterkörper von k. Wir dürfen

$$\wp\xi_\nu = a_\nu, \qquad \Sigma\xi_\nu = 0$$

annehmen. Der Index ν werde mod 3 genommen. Die Charakterwerte des Faktorensystems sind folgende:

$$\chi(g_{\sigma_{\nu-1},\sigma_\nu}) = 0, \quad \chi(g_{\sigma_\nu,\sigma_\nu}) = 1, \quad \chi(g_{\sigma_{\nu+1},\sigma_\nu}) = 1 .$$

Um die Formeln von W. I, 3 und W. I, 2 anwenden zu können, brauchen wir noch eine Hilfszahl C, deren Spur nicht verschwindet. Die Spur von $C = \Sigma\xi_{\nu+1}\xi_\nu$ ist 1. Nach leichter Rechnung folgt.

$$\delta_{\sigma_\nu} = \xi_{\nu+1} + 1 \quad (\delta_e = 0); \quad \wp\delta_{\sigma_\nu} = a_{\nu+1}; \quad \gamma = \Sigma a_{\nu+1}\xi_\nu .$$

Satz. *Durch*

$$K = R\left(\frac{a_2\xi_1 + a_3\xi_2 + a_1\xi_3 + r}{\wp}\right)$$

werden alle Körper mit Quaternionengruppe gegeben, die den biquadratischen Körper k *enthalten. Dabei durchläuft* r *alle Zahlen des Grundkörpers* R.

Zweiter Fall. Die Charakteristik des Grundkörpers sei $\neq 2$. $k = R(\xi_1, \xi_2, \xi_3)$ sei wieder ein Körper mit der Vierergruppe Γ, wobei

$$\xi_\nu^2 = a_\nu, \qquad \Pi \xi_\nu = 1$$

gelte. Wir behaupten den folgenden Satz.

Satz. *Damit es überhaupt Körper mit Quaternionengruppe gibt, die k enthalten, müssen die quadratischen Formen*

$$\Sigma a_\nu x_\mu^2 \quad \textit{und} \quad \Sigma y_\nu^2 \qquad (\mu, \nu = 1, 2, 3)$$

einander äquivalent sein. Umgekehrt, sind diese äquivalent, so sei

$$x_\mu = \sum_\nu p_{\mu\nu} y_\nu \qquad (|p_{\mu\nu}| = 1).$$

Dann werden durch

$$K = R(\sqrt{r(p_{11}\xi_1 + p_{22}\xi_2 + p_{33}\xi_3)})$$

alle solchen Körper geliefert. Dabei durchläuft r alle Zahlen $\neq 0$ des Grundkörpers R.

Beweis. Die Quaternionengruppe sei in Gestalt eines verschränkten Produktes gegeben:

$$i_\sigma i_\tau = \zeta_{\sigma,\tau} i_{\sigma\tau} \qquad (\zeta_{\sigma,\tau} = \pm 1;\ i_e = 1)$$

Ob k Unterkörper eines Quaternionenkörpers ist oder nicht, hängt ab vom Zerfall der Algebra $\mathfrak{A} = (\zeta_{\sigma,\tau}, k)$.

Wir formen jetzt die Algebra $\mathfrak{A}$ um. Dazu bezeichnen wir die Zahlen $1, \xi_1, \xi_2, \xi_3$ kurz mit ξ_σ, in der Weise, daß ξ_σ bei Anwendung des Automorphismus σ ungeändert bleiben soll. Ebenso schreiben wir $\xi_\sigma^2 = a_\sigma$. $\mathfrak{A}$ wird erzeugt von den Größen i_σ und $\xi_\tau i_\tau$. Es ist i_σ mit $\xi_\tau i_\tau$ vertauschbar. Die i_σ erzeugen das gewöhnliche Quaternionensystem $\mathfrak{Q}$, und die $\xi_\tau i_\tau$ erzeugen ein Untersystem $(-a_1, -a_2)$ in $\mathfrak{A}$. Daher ist

$$\mathfrak{A} \cong (-a_1, -a_2) \times \mathfrak{Q}.$$

Wenn $\mathfrak{A}$ zerfällt, so gibt es in $\mathfrak{Q}$ Größen $v_\mu = \sum_\nu p_{\mu\nu} i_\nu$ mit $v_\mu^2 = -\dfrac{1}{a_\mu}$, $v_1 v_2 v_3 = -1$. Es ist leicht zu sehen, daß die Substitution $x_\mu = \sum_\nu p_{\mu\nu} y_\nu$ die Determinante 1 hat und die Form $\Sigma a_\mu x_\mu^2$ in Σy_ν^2 überführt. Umgekehrt gibt eine solche Matrix $p_{\mu\nu}$ Anlaß zur Bildung der erwähnten Größen v_μ, und $\mathfrak{A}$ zerfällt dann.

Wir erweitern das System $\mathfrak{Q}$ mit dem Körper k und bilden im erweiterten System $\mathfrak{Q}_k$ die Größen $j_\sigma = \xi_\sigma v_\sigma$. Die j_σ haben dasselbe Faktorensystem wie die i_σ. Endlich setzen wir

$$C = \tfrac{1}{2} \sum_\sigma i_\sigma^{-1} j_\sigma$$
$$= \tfrac{1}{2}(1 + p_{11}\xi_1 + p_{22}\xi_2 + p_{33}\xi_3) + \tfrac{1}{2}(p_{32}\xi_3 - p_{23}\xi_2) i_1 + \tfrac{1}{2}(p_{13}\xi_1 - p_{31}\xi_3) i_2 + \tfrac{1}{2}(p_{21}\xi_2 - p_{12}\xi_1) i_3.$$

Es folgt $i_\tau^{-1} C j_\tau = C$. Mit $\mathrm{N}C$, $\mathrm{Sp}\, C$ sei hier die (reduzierte) Quaternionennorm bzw. Spur bezeichnet; $\bar{C}$ sei das zu C konjugierte Quaternion. Wegen

$$\mathrm{N}C = \tfrac{1}{2}\,\mathrm{Sp}\, C\bar{C} = \tfrac{1}{4}\,\mathrm{Sp}\, C \sum_\sigma \bar{j}_\sigma^{-1} i_\sigma = \tfrac{1}{4}\,\mathrm{Sp} \sum_\sigma i_\sigma^{-1} C i_\sigma = \mathrm{Sp}\, C$$

ist

$$\mathrm{N}C = 1 + p_{11}\xi_1 + p_{22}\xi_2 + p_{33}\xi_3 = \gamma$$

von Null verschieden, denn die Zahlen $1, \xi_1, \xi_2, \xi_3$ bilden eine Basis des Körpers k. Da C kein Nullteiler ist, gilt

$$C j_\tau C^{-1} = i_\tau.$$

Diese Gleichung bleibt richtig, wenn C durch $i_\sigma C^\sigma$ ersetzt wird; daraus folgt

$$i_\sigma C^\sigma = \delta_\sigma C$$

mit einer Zahl δ_σ aus dem Körper k; aus dieser Beziehung lassen sich die Zahlen δ_σ übrigens auch ohne Mühe berechnen. Setzen wir in der Identität

$$(CC^{-\sigma}) \cdot (CC^{-\tau})^{\sigma} \cdot (CC^{-\sigma\tau})^{-1} = 1$$

$CC^{-\sigma} = \delta_\sigma^{-1} i_\sigma$ usw. ein, so erscheint die Gleichung

$$\frac{\delta_\sigma \delta_\tau^{\sigma}}{\delta_{\sigma\tau}} = \zeta_{\sigma,\tau}\,.$$

Wir hatten vorhin $\mathrm{N}\,C = \gamma$ gesetzt; wird von der Gleichung $C^{\sigma} C^{-1} = i_\sigma^{-1}\,\delta_\sigma$ die Norm genommen, so folgt

$$\gamma^{\sigma-1} = \delta_\sigma^2\,.$$

Aus der allgemeinen Theorie übernehmen wir jetzt den Schluß, daß der Körper $K = k(\sqrt{\gamma}) = R(\sqrt{\gamma})$ ein Quaternionenkörper ist mit k als Unterkörper, und daß alle solchen Körper durch $R(\sqrt{r\gamma})$ gegeben werden. Dies wollten wir gerade beweisen. —

Für den Fall, daß R (und damit auch k) ein reeller algebraischer Zahlkörper ist, hat $\sqrt{\gamma}$ ein geometrische Bedeutung: Die Transformation der i_1, i_2, i_3 in die normierten v_1, v_2, v_3 (d. h. in die j_1, j_2, j_3) geschieht durch eine Drehung um eine gewisse Achse und um einen gewissen Winkel φ. Es ist dabei $\sqrt{\gamma} = 2\cos\frac{\varphi}{2}$.

Zm Schluß werde der historisch erste, von Dedekind [6]) angegebene Quaternionenkörper als Beispiel konstruiert: Die Form $2x_1^2 + 3x_2^2 + \frac{1}{6}x_3^2$ wird durch

$$(p_{\mu\nu}) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 1 & -1 & 2 \end{pmatrix}$$

in $\Sigma\, y_\nu^2$ übergeführt. Mit $r = 6$ erhalten wir den Körper

$$K = R\big(\sqrt{6 + 3\sqrt{2} + 2\sqrt{3} + 2\sqrt{2}\sqrt{3}}\big)\,.$$

K ist über dem Grundkörper R der rationalen Zahlen galoissch mit der Quaternionengruppe und enthält $k = R(\sqrt{2}, \sqrt{3})$ als Unterkörper [7]).

Göttingen, den 20. September 1935.

---

[6]) R. Dedekind, Konstruktion von Quaternionkörpern, Ges. Werke **2**, Braunschweig 1931.

[7]) Die Bedingungen für die Erweiterbarkeit eines biquadratischen Zahlkörpers mit Vierergruppe über dem rationalen Zahlkörper zu einem Quaternionenkörper wurden neuerdings auch von E. Rosenblüth in seiner Dissertation behandelt, allerdings mit unvollständigem Ergebnis. Siehe: Die arithmetische Theorie und die Konstruktion der Quaternionenkörper auf klassenkörpertheoretischer Grundlage, Monatshefte f. Math. u. Phys. **41** (1934).

Eingegangen 20. September 1935.

Über die sogenannte Hospitalsche Regel.

Von *Fritz Lettenmeyer* in München.

Der Grenzwert eines Quotienten zweier reeller Funktionen läßt sich bekanntlich in gewissen Fällen dadurch ermitteln, daß man an Stelle des Quotienten der beiden Funktionen den Quotienten ihrer Ableitungen untersucht, ein Verfahren, das gelegentlich als „Hospitalsche Regel" bezeichnet wird.

Für die Formulierung und den Beweis der Regel muß unterschieden werden, ob die Funktionen den Grenzwert Null oder einen unendlichen Grenzwert haben; unwesentlich ist, ob es sich um den Grenzübergang der unabhängigen Variablen gegen eine endliche oder eine unendliche Stelle handelt.

Wir wollen etwa folgenden Satz herausgreifen:

Für $x > x_0$ seien die reellen Funktionen $\varphi(x)$ und $\psi(x)$ differenzierbar und $\psi'(x) \neq 0$. Ferner gelte

$$\lim_{x \to +\infty} |\psi(x)| = +\infty, \quad \lim_{x \to +\infty} \frac{\varphi'(x)}{\psi'(x)} = A.$$

Dann folgt

$$\lim_{x \to +\infty} \frac{\varphi(x)}{\psi(x)} = A.$$

(*A darf auch $+\infty$ oder $-\infty$ sein.*)

Für diesen Satz geben die heute gebräuchlichen Lehrbücher der Differentialrechnung einen unnötig umständlichen Beweis, was daran liegt, daß als Ausgangspunkt stets der sogenannte erweiterte Mittelwertsatz der Differentialrechung

$$\frac{\varphi(x) - \varphi(a)}{\psi(x) - \psi(a)} = \frac{\varphi'(\xi)}{\psi'(\xi)} \qquad (a < \xi < x)$$

dient.

Es sei gestattet, hier einen besonders einfachen Beweis mitzuteilen.

Vorbemerkung. ψ' hat für $x > x_0$ konstantes Vorzeichen; denn hätte ψ' an zwei Stellen verschiedenes Vorzeichen, so gäbe es eine Zwischenstelle mit $\psi' = 0$ (Satz von Darboux über die Zwischenwerte einer Ableitung). Es darf also ohne Einschränkung der Allgemeinheit $\psi' > 0$ statt $\psi' \neq 0$ und damit $\psi \to +\infty$ statt $|\psi| \to +\infty$ angenommen werden.

Beweis. Ist $\varepsilon > 0$ vorgegeben, so gilt für hinreichend große x

$$A - \varepsilon < \frac{\varphi'}{\psi'} < A + \varepsilon,$$

oder (wegen $\psi' > 0$)

$$(1) \qquad (A - \varepsilon)\,\psi' < \varphi' < (A + \varepsilon)\,\psi';$$

es ist also

$\varphi - (A - \varepsilon)\,\psi$ monoton wachsend,
$\varphi - (A + \varepsilon)\,\psi$ monoton abnehmend.

Die Funktion $\varphi - (A - \varepsilon)\,\psi$ hat daher für $x \to +\infty$ entweder den Grenzwert $+\infty$ oder einen endlichen Grenzwert. Dasselbe gilt für die Funktion $\varphi - \left(A - \frac{\varepsilon}{2}\right)\psi$,

da in der bisherigen Überlegung ebensogut $\frac{\varepsilon}{2}$ wie ε stehen kann. Hätte nun die erstere Funktion einen endlichen Grenzwert, dann erst recht auch die letztere, da ψ von einer Stelle an positiv ist. Es würde nun durch Subtraktion folgen, daß auch $\frac{\varepsilon}{2}\psi$ einen endlichen Grenzwert hätte, im Widerspruch mit $\psi \to +\infty$. Es gilt also

$$\varphi - (A - \varepsilon)\psi \to +\infty .$$

Genau analog beweist man

$$\varphi - (A + \varepsilon)\psi \to -\infty .$$

Mithin ist für hinreichend große x

$$\varphi - (A - \varepsilon)\psi > 0 ,$$
$$\varphi - (A + \varepsilon)\psi < 0 ,$$

oder

$$A - \varepsilon < \frac{\varphi}{\psi} < A + \varepsilon ,$$

was die Behauptung ist. —

Man sieht sofort, daß bei $A = +\infty$ oder $-\infty$ der Beweis nur unwesentlich modifiziert zu werden braucht und daß er in der gleichen Form auch für $x \to x_0 - 0$ gilt.

Alle Fälle der Hospitalschen Regel, auch diejenigen, in welchen die Funktionen den Grenzwert Null haben, lassen sich nach der obigen Methode auf einheitliche Art beweisen.

Abgesehen von der Erschwerung des Beweises hat die erwähnte Verwendung des erweiterten Mittelwertsatzes auch noch einen methodischen Nachteil: Der Beweis versagt für einen Fall, in welchem die Behauptung auch noch richtig ist, nämlich für den Fall, daß $\psi'(x)$ „immer wieder" (d. h. für eine Menge von x-Werten mit der oberen Grenze $+\infty$) gleichzeitig mit $\varphi'(x)$ verschwinden darf, während sonst $\psi'(x) > 0$ ist und die Grenzwertbeziehung $\frac{\varphi'}{\psi'} \to A$ unter Ausschluß dieser Nullstellen zu verstehen ist. Im übrigen bleibt die Voraussetzung $\psi \to +\infty$.[1])

Diese Verallgemeinerung ist schon von Stolz[2]) bemerkt und bewiesen worden. Einen einfacheren Beweis als den Stolzschen hat Rouquet[3]) angegeben (zwar nur für $\psi(x) = x$, aber ohne weiteres auf den Fall eines beliebigen $\psi(x)$ übertragbar); der Rouquetsche Beweis ist leider nicht in die Lehrbücher übergegangen.

Der von mir oben angegebene Beweis bleibt auch unter diesen allgemeineren Voraussetzungen ohne weiteres gültig; man hat lediglich bis zu den Ungleichungen (1) die jetzt erlaubten gemeinsamen Nullstellen von φ' und ψ' auszunehmen und weiterhin an Stelle von (1) die Ungleichungen

$$(2) \qquad (A - \varepsilon)\psi' \leqq \varphi' \leqq (A + \varepsilon)\psi'$$

zu benützen, welche ja für alle hinreichend großen x gelten.

[1]) In Anwendungen kann man gelegentlich auf diese Verallgemeinerung angewiesen sein; s. z. B. meine Arbeit: Über das asymptotische Verhalten der Lösungen von Differentialgleichungen und Differentialgleichungssystemen, Sitz.-Ber. d. Bayer. Ak. d. Wiss., Math.-naturw. Abt., 1929, S. 230, Fußnoten 11 und 12.

[2]) Grundzüge der Differential- und Integralrechung **1** (1893), S. 82.

[3]) Nouv. Ann. de Math. (2) **16** (1877), S. 113—115.

Eingegangen 6. Oktober 1935.

Die Normen aus einer normalen Divisionsalgebra über einem algebraischen Zahlkörper.

Von *Helmut Hasse* in Göttingen und *Otto Schilling* z. Zt. in Princeton.

Sei A eine normale Divisionsalgebra vom Grade m über einem algebraischen Zahlkörper k. Wir behandeln in dieser Arbeit die Frage, welche Zahlen $\alpha \neq 0$ aus k Normen von Elementen aus A sind, Norm durchweg im reduzierten Sinne verstanden.

Wir beweisen die folgenden Tatsachen:

I. *Damit ein $\alpha \neq 0$ aus k Norm eines Elementes aus A ist, ist notwendig, daß α an allen unendlichen Verzweigungsstellen von A positiv ist.*

II. *Dies ist auch hinreichend, wenn m höchstens durch 2^1 teilbar ist oder wenn $m = 2^\mu m_0 (\mu > 1,\ 2 \nmid m_0)$ ist und k die 2^μ-ten Einheitswurzeln enthält.*

II′. *Allgemein ist für $4 \mid m$ α jedenfalls dann Norm eines Elementes aus A, wenn α an allen unendlichen Verzweigungsstellen von A positiv ist und an allen endlichen Verzweigungsstellen durch 2 teilbarer Ordnung von A eine durch 2 teilbare Ordnungszahl besitzt.*

Ob die letztere Bedingung im Falle $4 \mid m$ entbehrlich ist und somit durchweg allein die angegebenen Vorzeichenbedingungen maßgebend sind, können wir leider nicht entscheiden. Jedenfalls wird durch diese Sätze in einer großen Reihe von Fällen, z. B. durchweg für $2 \nmid m$, festgestellt, daß die Norm des allgemeinen Elementes von A, eine Form der Dimension m in m^2 Unbestimmten mit Koeffizienten aus k, eine *universelle Form* ist, d. h. alle $\alpha \neq 0$ aus k darstellt.

Im Falle $m = 2$ liefert II unter anderem die bekannte Tatsache, daß jede positive rationale Zahl als Summe von vier rationalen Quadratzahlen darstellbar ist (A die gewöhnliche Quaternionenalgebra).

Beweis von I.

Ist $\alpha = N(a)$ mit a aus A, so liegt a in einem maximal-kommutativen Teilkörper K von A, und nach der Theorie der Norm aus A besteht die Relation $\alpha = N(a)$ auch im Sinne der Norm aus K. Ist nun $\mathfrak{p}$ eine unendliche Verzweigungsstelle von A, so sind bekanntlich alle Primteiler $\mathfrak{P}$ von $\mathfrak{p}$ in K verzweigt, d. h. während $k_\mathfrak{p}$ reell ist, sind alle zugehörigen $K_\mathfrak{P}$ komplex. Dann ist aber $\alpha = N(a)$ positiv bei $\mathfrak{p}$.

Beweis von II und II′.

1. Ist Z ein über k zyklischer Körper vom Grade m, der A zerfällt, S ein erzeugender Automorphismus von Z, und

$$A = (\beta, Z, S) \tag{1}$$

eine zugehörige zyklische Erzeugung von A, also

$$A = Z(u) \tag{2}$$

mit

$$u^m = \beta \neq 0 \text{ in } k, \quad uzu^{-1} = z^S \quad (z \text{ in } Z), \tag{3}$$

so betrachten wir die speziellen Elemente

$$a = z(-u)^r \quad (z \text{ aus } Z) \tag{4}$$

aus A, deren Normen wegen $N(-u) = -\beta$ durch

$$N(a) = N(z)\,(-\beta)^r$$

gegeben sind.

Wir untersuchen dann, wann zu einem gegebenen $\alpha \neq 0$ aus k ein zyklischer Zerfällungskörper Z vom Grade m und damit eine zyklische Erzeugung (1) — (3) von A derart existiert, daß α Norm eines Elementes a aus A von der Form (4) ist. Diese Untersuchung geschieht durch Zurückführung der Fragestellung auf leicht angreifbare lokale Fragen für die Verzweigungsstellen von A mittels des allgemeinen Grunwaldschen Existenzatzes [1]).

Satz 1. *Damit zu einem gegebenen $\alpha \neq 0$ aus k und einem gegebenen r eine zyklische Erzeugung* (1) — (3) *von A derart existiert, daß α Norm eines Elementes a aus A von der Form* (4) *ist, ist notwendig und hinreichend, daß für jede Verzweigungsstelle $\mathfrak{p}$ von A ein m-ter Charakter $\chi_\mathfrak{p}$ von $k_\mathfrak{p}$ existiert mit den Eigenschaften:*

(5) *die Ordnung von $\chi_\mathfrak{p}$ ist durch den $\mathfrak{p}$-Index $m_\mathfrak{p}$ von A teilbar.*

(6) *Die Ordnung von $\chi_\mathfrak{p}((-1)^r\alpha)$ ist gleich $\dfrac{m_\mathfrak{p}}{(r, m_\mathfrak{p})}$.*

Beweis. a) *Notwendig.* Die Normsymbole $\chi_\mathfrak{p}(\xi) = \left(\dfrac{\xi, Z}{\mathfrak{p}}\right)$ liefern ein solches System von Charaktern $\chi_\mathfrak{p}$. Denn sie geben homomorphe Abbildungen der Multiplikationsgruppen der $k_\mathfrak{p}$ in die zyklische Galoisgruppe der Ordnung m von Z. Nach der arithmetischen Theorie der zyklischen Algebren [2]) gilt dabei einerseits (5), andererseits wegen der Voraussetzung $\alpha = N(a) = N(z)\,(-\beta)^r$ auch (6). Denn man hat

$$\chi_\mathfrak{p}((-1)^r\alpha) = \left(\frac{(-1)^r\alpha, Z}{\mathfrak{p}}\right) = \left(\frac{N(z)\,\beta^r, Z}{\mathfrak{p}}\right) = \left(\frac{\beta, Z}{\mathfrak{p}}\right)^r,$$

und $\left(\dfrac{\beta, Z}{\mathfrak{p}}\right)$ hat die Ordnung $m_\mathfrak{p}$.

b) *Hinreichend.* Nach (6) lassen sich die vorausgesetzten Charaktere $\chi_\mathfrak{p}$ so in einer festen zyklischen Gruppe $\{S\}$ der Ordnung m repräsentieren, daß dabei

$$\chi_\mathfrak{p}((-1)^r\alpha) = S^{r\mu_\mathfrak{p}} \tag{7}$$

wird, wo $\dfrac{\mu_\mathfrak{p}}{m}$ mod. 1 die $\mathfrak{p}$-Invarianten von A sind; denn $\dfrac{\mu_\mathfrak{p}}{m}$ hat mod. 1 die Ordnung $m_\mathfrak{p}$. Wir dürfen dabei neben den Verzweigungsstellen $\mathfrak{p}$ von A auch noch die etwa sonst noch in α vorkommenden Primstellen $\mathfrak{p}$ mitnehmen; für sie ist $\dfrac{\mu_\mathfrak{p}}{m} \equiv 0$ mod. 1, also genügt es, für sie $\chi_\mathfrak{p} = 1$ zu setzen. Nach dem Grunwaldschen Existenzsatz existiert dann ein zyklischer Körper Z vom Grade m über k mit den folgenden Eigenschaften:

---

[1]) W. Grunwald, Ein allgemeines Existenztheorem für algebraische Zahlkörper, Journ. f. Math. **169** (1933), 103—107.

[2]) H. Hasse, Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper, Math. Ann. **107** (1933), 731—760.

1. Bei einer geeigneten Darstellung der Galoisgruppe von Z als $\{S\}$ gilt

$$\left(\frac{\xi, Z}{\mathfrak{p}}\right) = \chi_{\mathfrak{p}}(\xi) \quad \text{für alle in } A \text{ verzweigten und alle in } \alpha \text{ vorkommenden Primstellen } \mathfrak{p}. \tag{8}$$

2. Außer dem hierdurch festliegenden Verzweigungsverhalten von Z für diese Primstellen $\mathfrak{p}$ ist Z nur noch an n weiteren Primstellen $\mathfrak{q}_i$ verzweigt, wenn $m = \prod_{i=1}^{n} l_i^{\mu_i}$ die Primzerlegung von m ist, und zwar von den Ordnungen $l_i^{\mu_i}$.

Nach (5), (8) ist dann Z Zerfällungskörper von A, also besteht eine zyklische Erzeugung (1) — (3) von A, und dabei ist

$$\left(\frac{\beta, Z}{\mathfrak{p}}\right) = S^{\mu_{\mathfrak{p}}} \qquad \text{für alle Primstellen } \mathfrak{p} \text{ von } k.$$

Nach (7), (8) hat man dann

$$\left(\frac{\alpha(-\beta)^{-r}, Z}{\mathfrak{p}}\right) = 1 \qquad \text{für alle in (8) genannten } \mathfrak{p}. \tag{9}$$

Ferner gilt (9) auch für alle übrigen $\mathfrak{p} \neq \mathfrak{q}_i$, denn für sie ist $\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = 1$, weil Z für $\mathfrak{p}$ unverzweigt ist und $\mathfrak{p}$ nicht in α vorkommt, sowie $\left(\frac{\beta, Z}{\mathfrak{p}}\right) = 1$, weil A für $\mathfrak{p}$ unverzweigt ist. Nach der Produktformel für das Normsymbol gilt daher (9) auch noch für die $\mathfrak{q}_i$, und somit für alle Primstellen $\mathfrak{p}$ von k. Daher ist

$$\alpha(-\beta)^{-r} = N(z) \quad \text{mit } z \text{ aus } Z,$$

also

$$\alpha = N(z)\,(-\beta)^r = N(z(-u)^r) = N(a) \qquad \text{mit } a = z(-u)^r \text{ aus } A\,.$$

Damit ist Satz 1 bewiesen.

2. Wir wenden jetzt Satz 1 an, um unter verschiedenen Voraussetzungen α als Norm aus A zu erweisen.

Satz 2. *Ist α prim zu allen endlichen und positiv an allen unendlichen Verzweigungsstellen von A, so ist α Norm aus A.*

Beweis. Wir wenden Satz 1 mit $r = 0$ an.

Dann lauten die Bedingungen (5), (6):

$$\chi_{\mathfrak{p}} \text{ hat durch } m_{\mathfrak{p}} \text{ teilbare Ordnung,}$$
$$\chi_{\mathfrak{p}}(\alpha) = 1\,.$$

Für eine endliche Verzweigungsstelle $\mathfrak{p}$ wird das unter der für α gemachten Voraussetzung durch den reinen Teilbarkeitscharakter

$$\chi_{\mathfrak{p}}(\xi) = \zeta^{\nu}, \text{ wenn } \xi \text{ bei } \mathfrak{p} \text{ die Ordnungszahl } \nu \text{ hat,}$$

(ζ primitive $m_{\mathfrak{p}}$-te Einheitswurzel) erfüllt, für eine unendliche Verzweigungsstelle $\mathfrak{p}$ ($m_{\mathfrak{p}} = 2$) durch den (einzigen) Nichthauptcharakter

$$\chi_{\mathfrak{p}}(\xi) = (-1)^{\nu}, \text{ wenn } \xi \text{ bei } \mathfrak{p} \text{ das Vorzeichen } (-1)^{\nu} \text{ hat}\,.$$

Satz 3. *Ist α von zu m primer Ordnungszahl an allen endlichen und positiv an allen unendlichen Verzweigungsstellen von A, so ist α Norm aus A.*

Beweis. Wir wenden Satz 1 mit $r = 1$ an. Dann lauten die Bedingungen (5), (6):

$$\chi_{\mathfrak{p}} \text{ hat durch } m_{\mathfrak{p}} \text{ teilbare Ordnung,}$$
$$\chi_{\mathfrak{p}}(-\alpha) \text{ hat die Ordnung } m_{\mathfrak{p}}.$$

Sie werden wieder durch die im Beweis von Satz 2 angegebenen Charaktere erfüllt.

Satz 4. *k enthalte die m-ten Einheitswurzeln. Ist dann α an allen unendlichen Verzweigungsstellen von A positiv, so ist α Norm aus A.*

Beweis. Wir wenden jetzt Satz 1 wieder mit $r = 0$ an, müssen aber für die endlichen Verzweigungsstellen $\mathfrak{p}$ andere Charaktere $\chi_\mathfrak{p}$ als bisher nehmen.

Auf Grund direkter Zerlegung der Charaktere entsprechend der Primzerlegung von m genügt es, die Existenz der fraglichen Charaktere $\chi_\mathfrak{p}$ unter der Voraussetzung zu beweisen, daß m eine Primzahlpotenz ist.

Nun existiert ein m-ter Charakter $\chi_\mathfrak{p}$ von $k_\mathfrak{p}$ mit durch $m_\mathfrak{p}$ teilbarer Ordnung und $\chi_\mathfrak{p}(\alpha) = 1$ sicher dann, wenn die Gruppe $k_\mathfrak{p}/k_\mathfrak{p}^m$ mindestens zwei unabhängige Elemente der Ordnung m besitzt; denn dann besitzt $k_\mathfrak{p}/\{\alpha, k_\mathfrak{p}^m\}$ noch mindestens ein Element der Ordnung m, also auch einen Charakter der Ordnung m. Es kommt also nur darauf an zu zeigen, daß $k_\mathfrak{p}/k_\mathfrak{p}^m$ unter der gemachten Voraussetzung über k mindestens zwei unabhängige Elemente der Ordnung m besitzt.

a) $\mathfrak{p} \nmid m$. Dann hat $k_\mathfrak{p}/k_\mathfrak{p}^m$ bekanntlich genau zwei unabhängige Elemente, nämlich repräsentiert durch

ein Primelement π zu $\mathfrak{p}$, Ordnung m,
eine Primitivwurzel ω mod. $\mathfrak{p}$, Ordnung $(m, \mathfrak{N}(\mathfrak{p}) - 1)$.

Wenn k die m-ten Einheitswurzeln enthält, ist aber $\mathfrak{N}(\mathfrak{p}) \equiv 1$ mod. m für jedes $\mathfrak{p} \nmid m$, und somit ist auch ω von der Ordnung m.

b) $\mathfrak{p} | m$. Ist n der (absolute) Grad von $k_\mathfrak{p}$, so hat die Gruppe $k_\mathfrak{p}/k_\mathfrak{p}^m$ nach Hensel [3]) den Typus $(m, \ldots, m, m_0)$, wo zuerst $(n+1)$-mal m steht (ein Primelement, n Einseinheiten unendlicher Ordnung in $k_\mathfrak{p}$) und dann noch ein weiteres uns hier nicht interessierendes $m_0 | m$ folgt; es genügt für unseren Zweck nach dem Gesagten, daß $n + 1 \geqq 2$ ist.

3. Mittels der Sätze 2—4 können wir jetzt den Beweis der eingangs ausgesprochenen Tatsachen II, II′ erbringen.

Beachtet man, daß für ein direktes Produkt $A = A_1 \times A_2$ zweier Algebren der Grade m_1, m_2 für jedes Elementpaar a_1 aus A_1, a_2 aus A_2 gilt

$$N_A(a_1 a_2) = N_{A_1}(a_1)^{m_2} N_{A_2}(a_2)^{m_1},$$

so reduzieren sich die in II, II′ ausgesprochenen Behauptungen auf folgende:

III. *Ist m prim zu 2, so ist jedes $\alpha \neq 0$ aus k Norm aus A.*

IV. *Ist $m = 2^\mu$ und enthält k die m-ten Einheitswurzeln, so ist jedes an allen Verzweigungsstellen von A positive $\alpha \neq 0$ aus k Norm aus A.*

Die Vorzeichenbedingung tritt natürlich nur für $\mu = 1$ auf, weil k für $\mu > 1$ total-komplex ist; und die Voraussetzung über k ist nur für $\mu > 1$ eine wirkliche Einschränkung.

IV′. *Allgemein ist für $m = 2^\mu$ ein $\alpha \neq 0$ aus k jedenfalls dann Norm aus A, wenn α für alle endlichen Verzweigungsstellen von A durch 2 teilbare Ordnungszahl hat und für alle unendlichen Verzweigungsstellen von A positiv ist.*

Die Richtigkeit von IV ist bereits durch Satz 4 als Spezialfall festgestellt.

Zum Beweis von III und IV′ bezeichne $\mathfrak{p}_i$ die endlichen Verzweigungsstellen von A. Ferner seien v_i (im Falle III) bzw. $2v_i$ (im Falle IV′) die Ordnungszahlen von α für die $\mathfrak{p}_i$. Wir wählen dann ein System von Zahlen π_i aus k, die genau durch $\mathfrak{p}_i^1$ teilbar,

[3]) K. Hensel, Allgemeine Theorie der Kongruenzklassengruppen und ihrer Invarianten in algebraischen Körpern, Journ. f. Math. **147** (1917), 1—15.